

The State of Texas

Executive Division
Capitol Building, 1E.8
P.O. Box 12697
Austin, Texas 78711-2697



Phone: 512-463-5770
Fax: 512-475-2761
Dial 7-1-1 For Relay Services
www.sos.texas.gov

Ruth R. Hughs
Secretary of State

February 4, 2020

Austin R. Evers
American Oversight

Sent via Electronic Mail in care of Clay M. Goode to: records@americanoversight.org

Re: Request for records, MULTI-20-0065-0069, received: January 21, 2020
(SOS PIR No. 20-0116)

Dear Mr. Evers:

This letter responds to your request for information under the Public Information Act, Chapter 552 of the Texas Government Code (the “PIA”), which was received by the Office of the Texas Secretary of State (the “Office”) via email on January 21, 2020 (the “Request”). In your Request, you indicate that you are seeking:

- 1. Any current policies, memoranda, or other guidance regarding the storage of records, both physical and electronic. This includes, but is not limited to, any current agency records retention schedule.*
- 2. Any current policies, memoranda, or other guidance regarding the automatic deletion of electronic records, including emails, documents, or other information stored electronically.*

We are processing your Request in accordance with the terms of the PIA. To that end, please find the attached information responsive to the portions of your Request seeking “[a]ny current policies . . . regarding the storage of records, both physical and electronic” and “[a]ny current policies . . . regarding the automatic deletion of electronic records, including emails, documents, or other information stored electronically.”

CLARIFICATION REQUEST/NOTICE OF APPLICATION OF SEC. 552.222

In order to fulfill the remainder of your Request—*i.e.*, “memoranda . . . or other guidance regarding the storage of records, both physical and electronic” and “memoranda . . . or other guidance regarding the automatic deletion of electronic records, including emails, documents, or other information stored electronically”—we need clarification regarding your inquiry. Clarifying or narrowing the scope of your request may help avoid the production of, and potential charges for, responsive information that you are not interested in receiving. It also may allow us to produce responsive documents to you more quickly. Additionally, we may be able to

avoid having to withhold certain information under the Public Information Act and seek a ruling from the Office of the Attorney General regarding the release of such records.

To that end, please clarify or narrow your inquiry by responding to the following questions:

1. It is unclear what you mean by “memoranda . . . or other guidance.” Are you requesting (1) *standalone documents*, such as employee procedures, policy manuals, and related guidance documents, regarding the storage or automatic deletion of agency records; (2) *e-mails or other written communications* reflecting the provision of guidance to Secretary of State employees regarding the storage or automatic deletion of agency records; or (3) both categories of information?
2. To the extent that your request for “memoranda . . . or other guidance” encompasses e-mails or other written communications:
 - a. Are you requesting (1) communications that were sent or provided *en masse* to all Secretary of State employees (or groups of employees) containing guidance regarding the storage or automatic deletion of agency records; (2) communications sent to *individual* Secretary of State employees containing guidance regarding the storage or automatic deletion of agency records; or (3) both categories of information?
 - b. Will you agree to narrow your inquiry to communications involving certain Secretary of State employees?¹ If so, please identify the employees (or categories of employees) covered by this portion of your Request. Narrowing your inquiry to a subset of Secretary of State employees would reduce the total time that we would have to spend responding to the remainder of your Request and, therefore, reduce—or potentially eliminate—any costs associated with processing the inquiry.²
 - c. Will you provide additional detail regarding the requested “memoranda . . . or other guidance”—including search terms for us to utilize—so that we can accurately identify and collect any responsive items?
3. What is the date range for the “memoranda . . . or other guidance” that you are seeking to obtain in this Request?

Depending on your clarification, we may have to provide you a statement of estimated costs pursuant to Section 552.2615 of the Texas Government Code. Likewise, providing the requested information may require programming and/or manipulation of data and would be available only at a cost that covers such programming or manipulation. *See* Tex. Gov’t Code § 552.231. In addition, some responsive information may be exempted from public disclosure under the PIA. However, we cannot make any of these determinations until we receive a clarified request from you.

¹ The Secretary of State’s office has approximately 180 employees across multiple divisions, each of which handles a wide variety of subject areas. For example, the Office’s Elections Division provides assistance and advice to Texas election officials on the proper conduct of elections. In addition, our Business and Public Filings Division’s responsibilities include receiving, filing, and maintaining myriad documents, including documents that create or affect business organizations and non-profit entities under Texas law, financing statements, and other documents provided for under the Uniform Commercial Code.

² We are amenable to working with you to determine an appropriate custodian set for the information you are seeking to obtain in this portion of the Request.

Under Section 552.222 of the PIA, if you do not respond in writing to this request for clarification within sixty-one days of this communication, your request for information is deemed by Texas law to be withdrawn. The Secretary of State is a strong supporter of open government, and this Office is ready and willing to respond to any and all public information requests. However, we must require that requests provide sufficient detail regarding the records being sought so that we may fulfill our duties under the PIA.

If you have any questions or need additional information, or if you would like to submit a clarified request, please contact our office at (512) 463-5770 or at the e-mail address listed below.

Sincerely,

A handwritten signature in blue ink, appearing to read 'Adam Bitter', is positioned above the typed name.

Adam Bitter
General Counsel
Office of the Texas Secretary of State
generalcounsel@sos.texas.gov

Enclosures



June 4, 2018

Mr. Vincent Houston
Director
Office of the Secretary of State
1019 Brazos, Room 439
Austin, TX 78701

Lorenzo de Zavala
State Archives and
Library Building

1201 Brazos Street
Austin, Texas
78701

P.O. Box 12927
Austin, Texas
78711-2927

www.tsl.texas.gov

Commission Chairman
Michael C. Waters

Members

Sharon T. Carr
F. Lynwood Givens
Larry G. Holt
Martha Wong

Director and Librarian
Mark Smith

Assistant State Librarian
Gloria Meraz

Re: Agency records retention schedule amendment approved for use.

Dear Mr. Houston:

Amendment 2 to your agency's 7th recertification of your records retention schedule is approved for use as of May 24, 2018. Your currently approved records retention schedule and all amendments are available on our website at <https://www.tsl.texas.gov/slrn/state/schedules.html>. Please maintain this amendment with your currently approved schedule so that it can be easily referenced.

We appreciate your efforts in maintaining an up-to-date schedule. Making additions and changes to your schedule as you identify them not only ensures the integrity of your recordkeeping practices, but keeps your agency in compliance with state regulations (13 TAC §6.4) requiring the submission of any needed amendments to a retention schedule during its certification period to keep the information in the schedule current.

We will notify you of the date your schedule is due for recertification. Any additional approved amendments to your schedule, such as this one, should be incorporated into your main retention schedule prior to submitting it for recertification.

Thank you again for your commitment to complying with state records management laws and regulations. If we can provide any assistance to you, please contact the Government Information Analyst assigned to your agency, Erica Wilson-Lang, at 512-463-6627 or ewilson@tsl.texas.gov.

Sincerely,

Craig Kelso
Director and State Records Administrator

cc: Agency head

TSLAC

Preserving yesterday
Informing today
Inspiring tomorrow

MULTI-TX-SOS-20-0065-A-000001



STATE OF TEXAS

Records Retention Schedule Certification

SLR 105C

Form SLR 105 or SLR 122 must accompany all submissions of this form.

Section 1. Agency Information

(Submitting agencies complete this section only)

Agency Code 307

Agency Name Secretary of State

(Check one)

- Initial Certification - Form SLR 105
Recertification - Form SLR 105
Amendment - Form SLR 122

I hereby certify that this records retention schedule was prepared in accordance with Texas Government Code, Chapter 441, Subchapter L.

(Check one)

- Agency Head
Records Management Officer

Signature

Vincent Houston

Name (Print or type)

Vincent Houston

Date

02/20/2018

Section 2. Approvals

(Submitting agencies do not write in this section)

State Auditor's Office

(For the exclusive use of the State Auditor's Office)

Signature

Name (Print or type)

Date

Not Required at This Time

Texas State Library and Archives Commission

(For the exclusive use of the State Library and Archives Commission)

Signature

Gloria Mera

Name (Print or type)

Gloria Mera

Date

5/24/18

Cert/Recert No.

7

Amendment No.

2

CAUTION

A state record whose retention period has expired may not be destroyed if any litigation, claim, negotiation, audit, public information request, administrative review, or other action involving the record is initiated; its destruction shall not occur until the completion of the action and the resolution of all issues that arise from it.

A state record whose retention period expires during any litigation, claim, negotiation, audit, public information request, administrative review, or other action involving the record may not be destroyed until the completion of the action and the resolution of all issues that arise from it.





STATE OF TEXAS
Records Retention Schedule

SLR 122
Rev. 2017-07

Retention Codes (field 7)

AC – See field 9 for specific records series definition
AV – Administratively valuable
CE – Calendar year end

FE – Fiscal year end
LA – Life of Asset
PM – Permanent
US – Until Superseded

Archival Codes (Field 10)

A/I – Transfer to State/University Archivist
R/O – Review by State/University Archivist

1. Agency Code: 307		2. Agency Name: Secretary of State											
3. Agency Item No.	4. Record Series Item No.	5. Record Series Title	6. Description	7. Ret. Code	8. Retention Period			9. AC Definition	10. Archival	11. Remarks	12. Legal Citations	13. N, C, O	14. Current AIN
					Years	Months	Days						
												O	32.20
32.21	2.2.012	Files Processed by Voter Registration System	Jury Management, Voter Registration, Voter List Maintenance, or Voting History Data files	AV								N	
34.50	1.1	Candidate Applications		AC	2			AC = Date of the election for which the application is made			Sec. 141.036, Texas Election Code	N	
33.60	1.1	Primary Finance Files		CE	7							C	33.60



November 13, 2015

Mr. Vincent Houston
Director
Texas Secretary of State
1019 Brazos
RM 439
Austin, TX 78701

State and Local
Records Management

Re: Agency records retention schedule amendment approved for use

Dear Mr. Houston:

P.O. Box 12927
Austin, Texas
78711.2927

Amendment 1 to your agency's 7th recertification of your records retention schedule is approved for use as of Friday, October 23, 2015. Your currently approved records retention schedule and all amendments are available on our website at <https://www.tsl.texas.gov/slrn/state/schedules.html>. Please maintain this amendment with your currently approved schedule so that it can be easily referenced.

4400 Shoal Creek Blvd.
Austin, Texas
78756

We appreciate your efforts in maintaining an up-to-date schedule. Making additions and changes to your schedule as you identify them not only ensures the integrity of your recordkeeping practices, but keeps your agency in compliance with state regulations (13 TAC §6.4) requiring the submission of any needed amendments to a retention schedule during its certification period to keep the information in the schedule current.

www.tsl.texas.gov

We will notify you of the date your schedule is due for recertification. Any additional approved amendments to your schedule, such as this one, should be incorporated into your main retention schedule prior to submitting it for recertification.

Commission Chairman
Michael C. Waters

Thank you again for your commitment to complying with state records management laws and regulations. If we can provide any assistance to you, please contact the Government Information Analyst assigned to your agency, Erica Wilson, at 512-463-6627 or ewilson@tsl.texas.gov.

Members
Sharon T. Carr
Martha Doty Freeman
F. Linwood Givens
Larry G. Holt
Wm. Scott McAfee
Sandra J. Pickett

Sincerely,

Craig Kelso
Director and State Records Administrator

Director and Librarian
Mark Smith

Assistant State Librarian
Edward Seidenberg

cc: State Auditor, State Archivist, Carlos H. Cascos

*Preserving yesterday,
informing today,
inspiring tomorrow.*

R01.307/307

307 EW



STATE OF TEXAS Records Retention Schedule Certification

SLR 105C

Form SLR 105 or SLR 122 must accompany all submissions of this form.

Section 1. Agency Information *(Submitting agencies complete this section only)*

Agency Code 307
Agency Name Secretary of State

(Check one)

- Initial Certification - Form SLR 105
- Recertification - Form SLR 105
- Amendment - Form SLR 122

I hereby certify that this records retention schedule was prepared in accordance with Texas Government Code, Chapter 441, Subchapter L.

(Check one)

- Agency Head
- Records Management Officer

Signature Vincent Houston
Name *(Print or type)* Vincent Houston
Date August 17, 2015

Section 2. Approvals *(Submitting agencies do not write in this section)*

State Auditor's Office
(For the exclusive use of the State Auditor's Office)

Signature _____
Name *(Print or type)* _____
Date _____

Not Required at This Time

Texas State Library and Archives Commission
(For the exclusive use of the State Library and Archives Commission)

Signature Donna Osborne
Name *(Print or type)* Donna Osborne
Date 10/23/15

Cert/Recert No. 7 Amendment No. 1

CAUTION

A state record whose retention period has expired may not be destroyed if any litigation, claim, negotiation, audit, public information request, administrative review, or other action involving the record is initiated; its destruction shall not occur until the completion of the action and the resolution of all issues that arise from it.

A state record whose retention period expires during any litigation, claim, negotiation, audit, public information request, administrative review, or other action involving the record may not be destroyed until the completion of the action and the resolution of all issues that arise from it.





STATE OF TEXAS

Records Retention Schedule Amendment

SLR 122
Form SLR 105C must accompany this form.

1. Page 1 of 1

2. Agency Code		307		3. Agency Name							Secretary of State		
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival		10. 106 No.	11. Current Schedule		12. Amend. Type		
			Agency	Storage	Total	9. Remarks	Page No.		Agency Item No.				
1.3.001	13.61	Bound Session Laws aka General & Special Laws of Texas	PM		PM	Refers only to bound volumes 81 st session and prior.		44	16.10	C			

Retention Codes (Field 7)			Archival Codes (Field 8)		Amendment Codes (Field 12)	
AC – After Closed, Terminated, Completed, Expired, Settled	CE – Calendar Year End	MO – Months	A – Transfer to State Archives	N – New		
AV – Administrative Value	FE – Fiscal Year End	PM – Permanent	R – Review by State Archivist	C – Changed		
	LA – Life of Asset	US – Until Superseded		D – Deleted		

Instructions for Completing Form SLR 122

Forms SLR 122 must be used by all state agencies to submit an amendment to an approved (certified/recertified) agency records retention schedule (Texas Government Code, Chapter 441, §441.185). See Form SLR 105C instructions for submission procedures. If you have questions relating to completion of this form or SLR 105C, please contact the State and Local Records Management Division at 512-463-7610.

Formatting: When duplicating this form electronically, leave at least ¾ inch in the top and left margins. Use 10 point font and larger for the data entered into the schedule.

Field 1 Enter the page number and the total number of pages in this amendment (i.e., 1 of 15).

Field 2 Enter the 3-digit Agency Code assigned by the Comptroller of Public Accounts.

Field 3 Enter the complete name of your agency.

Note For Fields 4 - 12

New Records Series: Enter all information for fields 4 – 10, leave field 11 blank, complete field 12.

Changed Records Series: Enter all information for fields 4 – 12.

Deleted Records Series: Leave fields 4 – 9 blank, complete field 10 if applicable, complete fields 11 - 12.

Field 4 Enter the item number for the records series from the *State Records Retention Schedule* (RRS). If the records series title is not included in the RRS, enter the numbers of the appropriate "Category" and "Section" from the RRS where it should be listed. Category and Section Numbers are at the top of the page in the RRS. If the records series cannot be matched to a category and section, then leave Field 4 blank.

Field 5 Enter the number that has been assigned by your agency to the corresponding records series. Do not assign an agency item number that is assigned to another records series on the approved (certified/recertified) retention schedule.

Field 6 Enter the official title of the records series (i.e., W-4 Forms, Labor Statistics Report, Surety Bonds).

Field 7 Enter the retention period of the records series is to be retained in active use at the agency, the number of years it is to be retained in an inactive storage facility, such as the State Records Center, and the total of the two amounts. If a retention period is less than one year, enter the number of months. Refer to the retention codes at the bottom of the form.

Field 8 Using the archival codes at the bottom of the form, indicate the archival value, if applicable, of the records series:

A - Used with records series that will be transferred to the State Archives and do not require a prior review by the State Archivist.

R - Used with records series that have undetermined archival value, and require a review by the State Archivist prior to being transferred to the State Archives.

Field 9 Enter any statute references, other legal citations, or agency policy used as a basis for the retention period.

Field 10 If this records series is stored at the State Records Center, enter the RMD 106 Storage Approval Number.

Field 11 If this records series amends an item on the current approved (certified/recertified) agency retention schedule, list the page number of the agency item number of the records series being amended. If the records series is new, leave blank. If the records series is being deleted, enter the page number and agency item number of the records series being deleted.

Field 12 Designate how *this* records series is being amended, a new records series, a changed records series, or a deleted records series. Refer to the amendment codes at the bottom of the form.



July 16, 2015

Mr. Vincent Houston
Director
Texas Secretary of State
1019 Brazos
RM 439
Austin, TX 78701

State and Local
Records Management

P.O. Box 12927
Austin, Texas
78711.2927

4400 Shoal Creek Blvd.
Austin, Texas
78756

www.tsl.texas.gov

Commission Chairman
Michael C. Waters

Members
Sharon T. Carr
Martha Doty Freeman
F. Linwood Givens
Larry G. Holt
Wm. Scott McAfee
Sandra J. Pickett

Director and Librarian
Mark Smith

Assistant State Librarian
Edward Seidenberg

*Preserving yesterday,
informing today,
inspiring tomorrow.*

RE: Agency records retention schedule approved for use

Dear Mr. Houston:

Your agency's records retention schedule is approved for use as of July 10, 2015. Your currently approved records retention schedule is available on our website at <https://www.tsl.texas.gov/slrn/state/schedules.html>. Please ensure all old copies of the schedule are superseded with this recertified copy.

Your approved retention schedule provides you with continuing authorization to dispose of agency records according to its terms. Please note that state regulations (13 TAC §6.8) require documentation of the final disposition of records by your agency. This requirement may be met by maintaining a disposition log or other evidence of the records series titles, dates covered, volume, and date of disposition. We urge on you the importance of disposing of the records of your agency in a timely manner in accordance with the retention periods on your schedule. The destruction of any records of your agency not on your schedule requires special authorization from us.

Each agency schedule must be reviewed, updated and submitted for recertification annually for the first two years after the initial approval of the schedule and every five years thereafter. The deadline for submission of your schedule for its next recertification is the last working day of **July 2020**.

During a certification period changes may need to be made to your schedule. State regulations (13 TAC §6.4) also allow for the submission of amendments to the retention schedule as needed to keep the information in the schedule current. If you are not familiar with the amendment process, or if you have any other questions, please contact the Government Information Analyst assigned to your agency, Erica Wilson, at 512-463-6627 or ewilson@tsl.texas.gov.

Your efforts in developing a records retention schedule are appreciated. It not only helps to ensure the integrity of your recordkeeping practices, but it is also essential to the success of your records management program.

Sincerely,

A handwritten signature in blue ink, appearing to read "CK" or "Craig Kelso".

Craig Kelso
Director and State Records Administrator

cc: State Auditor, State Archivist, Nandita Berry

FW



Texas State Library and Archives Commission

STATE OF TEXAS Records Retention Schedule Certification

SLR 105C

Form SLR 105 or SLR 122 must accompany all submissions of this form.

Section 1. Agency Information

(Submitting agencies complete this section only)

Agency Code 307

Agency Name Texas Secretary of State

(Check one)

- Initial Certification - Form SLR 105
- Recertification - Form SLR 105
- Amendment - Form SLR 122

I hereby certify that this records retention schedule was prepared in accordance with Texas Government Code, Chapter 441, Subchapter L.

(Check one)

- Agency Head
- Records Management Officer

Signature Vincent Houston

Name (Print or type) Vincent Houston

Date 02/05/15

Section 2. Approvals

(Submitting agencies do not write in this section)

State Auditor's Office

(For the exclusive use of the State Auditor's Office)

Signature _____

Name (Print or type) _____

Date _____

Not Required at This Time

Texas State Library and Archives Commission

(For the exclusive use of the State Library and Archives Commission)

Signature E. Hildeberg

Name (Print or type) _____

Date 02-10-15

Cert/Recert No. 7 Amendment No. —

CAUTION

A state record whose retention period has expired may not be destroyed if any litigation, claim, negotiation, audit, public information request, administrative review, or other action involving the record is initiated; its destruction shall not occur until the completion of the action and the resolution of all issues that arise from it.

A state record whose retention period expires during any litigation, claim, negotiation, audit, public information request, administrative review, or other action involving the record may not be destroyed until the completion of the action and the resolution of all issues that arise from it.





STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 1 of 75

2. Agency Code 307		3. Agency Name Secretary of State							
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.
			Agency	Storage	Total				
1.1	20.00	Administrative Files	AC	3	AC+3	R	AC=No longer of administrative value.	90-307-017	
1.1.008	20.10	Correspondence – General	2		2				

Retention Codes (Field 7)

AC – After Closed, Terminated, Completed, Expired, Settled
 AV – Administrative Value

CE – Calendar Year End
 FE – Fiscal Year End

LA – Life of Asset
 MO – Months

PM – Permanent
 US – Until Superseded

Archival Codes (Field 8)

A – Transfer to State Archives
 R – Review by State Archivist



STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 2 of 75

2. Agency Code 307		3. Agency Name Secretary of State							
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.
			Agency	Storage	Total				

1	13.80	Local Option Elections	10		10				
1	13.80-M1	Local Option Elections (Master)	0	AC+50	AC+50		Master at SRC. AC = Date of Microfilming.	92-307-141	
1	13.80-M2	Local Option Elections (Dup.)	AC+50		AC+50		Dup. at agency. AC=Date of Microfilming.		
5.1.004	30.00	Address & Telephone Listing	US		US				
1.1.007	30.10	Correspondence - Administrative	CE+5		CE+5	R			
1.1.008	30.20	Correspondence - General	CE+5		CE+5				
5.1.015	30.30	Correspondence Logbooks	1		1				
1.1.010	30.40	Office Procedures Memos	US+1		US+1				
1.1.013	30.50	Desk Calendars/Appointment Books Desk calendars, appointment books, and similar records, purchased with state funds, that document appointments, itineraries, and other activities of an agency official or employee.	CE+1		CE+1	R			
1.1.014	30.60	SOS Legal Opinions & Advice	5		5	R			

Retention Codes (Field 7)

Archival Codes (Field 8)

AC – After Closed, Terminated, Completed, Expired, Settled
AV – Administrative Value

CE – Calendar Year End
FE – Fiscal Year End

LA – Life of Asset
MO – Months

PM – Permanent
US – Until Superseded

A – Transfer to State Archives
R – Review by State Archivist



STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 3 of 75

2. Agency Code 307		3. Agency Name Secretary of State								
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.	
			Agency	Storage	Total					
1.1.058	30.70	Meeting Minutes Includes agenda	PM		PM	A	Elections Advisory Task Force, copy sent to State Archives.			
1.1.019	30.80	News or Press Releases	2		2	R				
1.1.020	30.90	Open Records Requests – Approved	AC+1		AC+1		AC = After request is approved.			
1.1.021	31.00	Open Records Requests – Denied	AC+2		AC+2		AC = After request is denied.			
1.1	31.10	Justice Department Submissions Section 5, Voting Rights Act	PM		PM		Paper filmed every 2 years. Paper and film retained in agency.			
1.1	31.10-M	Justice Department Submissions	PM	PM	PM		Used by public, vital record protection. Master at SRC. Dup. at agency.	91-307-090		
1.1	31.20	Legislative Tracking	AC+2	2	AC+4		AC = After close of the legislative Session.	91-307-084		
1.3.002	31.30	Publication Files	AV		AV	R				

Retention Codes (Field 7)

AC – After Closed, Terminated, Completed, Expired, Settled
AV – Administrative Value

CE – Calendar Year End
FE – Fiscal Year End

LA – Life of Asset
MO – Months

PM – Permanent
US – Until Superseded

Archival Codes (Field 8)

A – Transfer to State Archives
R – Review by State Archivist



STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 4 of 75

2. Agency Code 307		3. Agency Name Secretary of State								
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.	
			Agency	Storage	Total					
1.3.001	31.40	Elections Division Publications Record copy	PM		PM		Copies to Texas State Publications Depository Program, TSLAC.			
1.1.067	31.60	Reports - Administrative	3		3	R				
1.1.067	31.70	Special/Non-routine Reports	3		3	R				
1.1.070	31.80-F	Rules & Regulations (Final)	US+3		US+3	R				
1.1.071	31.80-W	Rules & Regulations (Working Files)	US+3		US+3	R				
5.4.013	31.90	Disaster Recovery Plan	US		US					
1.2.003	32.00	Forms History File Election Forms	AC+1		AC+1		AC = Discontinuance of use of form.			
1.2.006	32.10	Records Transmittal Forms	AC+2		AC+2		AC = Date of authorization for destruction, permanent transfer from storage, or transfer to the Archives and Information Services Division, Texas State Library and Archives Commission, by an agency records manager.			

Retention Codes (Field 7)				Archival Codes (Field 8)	
AC – After Closed, Terminated, Completed, Expired, Settled	CE – Calendar Year End	LA – Life of Asset	PM – Permanent	A – Transfer to State Archives	
AV – Administrative Value	FE – Fiscal Year End	MO – Months	US – Until Superseded	R – Review by State Archivist	



STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 5 of 75

2. Agency Code 307		3. Agency Name Secretary of State								
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.	
			Agency	Storage	Total					
2.2.011	32.20	Batch/data Entry Control Form Voter Registration	AC		AC	Used to track transmittal of voter registration tapes received from counties. AC = When reconciliation confirmed.				
2.2.012	32.30	Error Reject Reports	AV		AV					
1	32.40	Hispanic Surname Printout	AV		AV	AC = After the company has been Certified.				
2.2	32.50	Certification of Data Processing Companies	AC+1		AC+1					
4.1.002	32.60	Billing Detail	FE+3		FE+3					
4.2.001	32.70	Cash Deposit Vouchers	FE+3		FE+3					
4.2.002	32.80	Cash Receipts	FE+3		FE+3					
4.2.003	32.90	Daily Cash Receipt Log	FE+3		FE+3					
4.2.005	33.00	Purchase Voucher Voter Registration, Chapter 19	FE+3		FE+3					

Retention Codes (Field 7)

AC – After Closed, Terminated, Completed, Expired, Settled
AV – Administrative Value

CE – Calendar Year End
FE – Fiscal Year End

LA – Life of Asset
MO – Months

PM – Permanent
US – Until Superseded

Archival Codes (Field 8)

A – Transfer to State Archives
R – Review by State Archivist



STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 6 of 75

2. Agency Code 307		3. Agency Name Secretary of State							
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.
			Agency	Storage	Total				

4.2.007	33.10	Expenditure Voucher Postage permit for counties	FE+3		FE+3				
5.2.010	33.20	Equipment Manuals	LA		LA				
1	33.30	Election Inspector Files	CE+5	5	CE+10	A		91-307-085	
1	33.40	County Precinct Maps	CE+10		CE+10	A	Section 42.037, Texas Election Code		
1	33.50	Election Returns – Precinct by Precinct	CE	10	CE+10	A	Paper filmed. Paper retained until CE then sent to SRC.	98-307-219	
1	33.50-M	Election Returns – Precinct by Precinct	PM	PM	PM		For public use, vital records protection. Master at SRC. Dup. at agency.	92-307-168	
1	33.60	Primary Finance Files	CE+2	5	CE+7	E	Archival review code removed subsequent to internal appraisal by the Archives and Information Services Division, TSLAC, Dec. 15, 1998.	91-307-066	
1	33.70	Petition to Place Nominees on General Election Ballot	CE+2		CE+2				

Retention Codes (Field 7)

AC – After Closed, Terminated, Completed, Expired, Settled
AV – Administrative Value

CE – Calendar Year End
FE – Fiscal Year End

LA – Life of Asset
MO – Months

PM – Permanent
US – Until Superseded

Archival Codes (Field 8)

A – Transfer to State Archives
R – Review by State Archivist



STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 7 of 75

2. Agency Code 307		3. Agency Name Secretary of State								
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.	
			Agency	Storage	Total					
1	33.80	Voter Registration Information Request Forms	1		1					
1	33.90	Independent Candidates for President on the General Election Ballot	2		2					
1	33.90-M	Independent Candidates for President on the General Election Ballot	0	CE+10	CE+10		Master at SRC. Dup. at agency for CE+10.	93-307-189		
1	34.00	Certification of Voting Equipment	PM		PM					
1	34.10	Precinct by Precinct Voter Registrations	20		20	R	Paper filmed. Paper retained until microfilmed.			
1	34.10-M	Precinct by Precinct Voter Registrations	PM	PM	PM		Master at SRC. Dup. at agency.	94-307-196		
1	34.20	Political Party Rules	10		10	R				
1.1.043	34.30	Training Materials Election Officials	US+1		US+1					

Retention Codes (Field 7)

AC – After Closed, Terminated, Completed, Expired, Settled
AV – Administrative Value

CE – Calendar Year End
FE – Fiscal Year End

LA – Life of Asset
MO – Months

PM – Permanent
US – Until Superseded

Archival Codes (Field 8)

A – Transfer to State Archives
R – Review by State Archivist



STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 8 of 75

2. Agency Code 307		3. Agency Name Secretary of State								
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.	
			Agency	Storage	Total					
1	34.40	Election Returns – County by County	CE	10	CE+10	A	Paper filmed. Paper retained until CE then sent to SRC.	98-307-220		
1	34.40-M	Election Returns – County by County	PM	PM	PM		For public use, vital records protection. Master at SRC. Dup. at agency.	92-307-167		

Retention Codes (Field 7)				Archival Codes (Field 8)					
AC – After Closed, Terminated, Completed, Expired, Settled	CE – Calendar Year End	LA – Life of Asset	PM – Permanent	A – Transfer to State Archives	AV – Administrative Value	FE – Fiscal Year End	MO – Months	US – Until Superseded	R – Review by State Archivist



STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 9 of 75

2. Agency Code 307		3. Agency Name Secretary of State							
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.
			Agency	Storage	Total				
5.1.012	40.00	Charge Schedules – Price Lists	US+3		US+3		Electronic kept until US.		
1.1.007	40.10	Correspondence – Administrative	4		4	R	Division Correspondence.		
1.1.070	40.30	Standards Manual (Final)	US+3		US+3	R	Division Standards.		
1.1.071	40.30-W	Standards Manual (Working Files)	US+3		US+3	R			
1.1.043	40.40	Training Materials	US+1		US+1				
5.4.013	40.50	Disaster Recovery Plan	US		US		Recovery Procedures.		
2.1.002	40.60	Automated Files – Masters	AC		AC		Back-up Storage – Mainframe, AC = Completion of 3 rd update cycle except for: a) Data file which replaces or serves in lieu of a textual record – Follow the retention period approved for the equivalent type of textual record. b) Output data file extracted from system solely to produce printed reports or other publications – Dispose of when no longer needed to create report or publication.		

Retention Codes (Field 7)

AC – After Closed, Terminated, Completed, Expired, Settled
AV – Administrative Value

CE – Calendar Year End
FE – Fiscal Year End

LA – Life of Asset
MO – Months

PM – Permanent
US – Until Superseded

Archival Codes (Field 8)

A – Transfer to State Archives
R – Review by State Archivist



STATE OF TEXAS Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 10 of 75

2. Agency Code 307		3. Agency Name Secretary of State						
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	10. 106 No.	11. TSLAC ONLY Amend. No.
			Agency	Storage	Total	9. Remarks		

2.1.002	40.70	Automated Files	AC		AC	Mini/Micro AC = Completion of 3 rd update cycle except for: a) Data file which replaces or serves in lieu of a textual record – Follow the retention period approved for the equivalent type of textual record. b) Output data file extracted from system solely to produce printed reports or other publications – Dispose of when no longer needed to create report or publication.		
2.2.012	40.80	Computer Produced Output	AV		AV			
2.1.009	40.90	Documentation	AC		AC	AC = Until electronic records are transferred to and made usable in a new hardware or software environment with new documentation or there are no electronic records being retained to meet an approved retention period that require the documentation to be retrieved and read. 13 TAC 6.97(a)		

Retention Codes (Field 7)				Archival Codes (Field 8)			
AC – After Closed, Terminated, Completed, Expired, Settled	CE – Calendar Year End	LA – Life of Asset	PM – Permanent	A – Transfer to State Archives			
AV – Administrative Value	FE – Fiscal Year End	MO – Months	US – Until Superseded	R – Review by State Archivist			



STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 11 of 75

2. Agency Code 307		3. Agency Name Secretary of State							
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.
			Agency	Storage	Total				

2.1.007	41.00	Programs	AC		AC	AC = Until electronic records are transferred to and made usable in a new software environment or there are not electronic records being retained to meet an approved retention period that require the software to be retrieved and read. 13 TAC 6.97(a)		
2.2.004	41.10	Job Schedules	3MO		3MO	Electronic kept until US.		
2.2.010	41.20	Data Processing Planning	US+3		US+3			
4.1.002	41.30	Billing of Services	FE+3		FE+3			
4.2.003	41.40	Daily Cash Receipts Log	FE+3		FE+3			
4.2.007	41.50	Expenditure Voucher	FE+3		FE+3			
1.2.013	41.70	Microfiche Masters	US+1		US+1			

Retention Codes (Field 7)	Archival Codes (Field 8)
AC – After Closed, Terminated, Completed, Expired, Settled AV – Administrative Value	A – Transfer to State Archives R – Review by State Archivist
CE – Calendar Year End FE – Fiscal Year End	PM – Permanent US – Until Superseded
LA – Life of Asset MO – Months	



STATE OF TEXAS Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 12 of 75

2. Agency Code 307		3. Agency Name Secretary of State							
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.
			Agency	Storage	Total				
1.1.069	1.01	Weekly Activity Reports	FE+2		FE+2				
1.1.006	1.02	Complaint Letters	AC+3		AC+3		AC = Problem Solved.		
1.1.007	1.03	Administrative Correspondence	AC+4		AC+4	R	Record Copy AC = Purpose of record has been fulfilled. AC = Purpose of record has been fulfilled.		
1.1.057	1.04	Internal Transitive Correspondence	AC		AC				
1.1.027	1.05	Proposed Legislation	FE+2		FE+2				
1.1.010	1.06	General UCC Management Information	US+3		US+3				
1.1.014	1.07	A.G. Opinion	AV		AV	R	CAUTION: Does not include legal opinion or advice rendered on a matter in litigation or with regard to pending litigation. See item #1.1.048.		
1.1.008	1.08	General Correspondence	AC+3		AC+3		AC = Purpose of record has been Fulfilled.		
1.1	1.10	Change of Address	CE+1		CE+1				

Retention Codes (Field 7)

AC – After Closed, Terminated, Completed, Expired, Settled
AV – Administrative Value

CE – Calendar Year End
FE – Fiscal Year End

LA – Life of Asset
MO – Months

PM – Permanent
US – Until Superseded

Archival Codes (Field 8)

A – Transfer to State Archives
R – Review by State Archivist



STATE OF TEXAS Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 13 of 75

2. Agency Code 307		3. Agency Name Secretary of State							
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.
			Agency	Storage	Total				
1.1.008	1.14	Correspondence Hot Checks	FE+2		FE+2				
1.1.008	1.15	Correspondence with Sections	AC+2		AC+2		AC = Purpose of record has been Fulfilled.		
1.1	1.16	Information Forwarded to County Clerk Offices	PM		PM				
1.1	1.17	Form Companies Approved/Not Approved	US		US				
1.1	1.17-M	Form Companies Approved/Not Approved Film Tests	AV		AV				

Retention Codes (Field 7)

AC – After Closed, Terminated, Completed, Expired, Settled
AV – Administrative Value

CE – Calendar Year End
FE – Fiscal Year End

LA – Life of Asset
MO – Months

PM – Permanent
US – Until Superseded

Archival Codes (Field 8)

A – Transfer to State Archives
R – Review by State Archivist



STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 14 of 75

2. Agency Code	307	3. Agency Name Secretary of State						
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	10. 106 No.	11. TSLAC ONLY Amend. No.
			Agency	Storage	Total	9. Remarks		

1.1.008	1.19	Correspondence for Elections	FE+5		FE+5			
1.1.008	1.20	Building Correspondence	3		3			
1.1.067	1.21	Consulting Firms Reports	US+3		US+3	R		
1.1.008	1.22	Moore Business Forms/Reject Letters	US+5		US+5			
1.1.008	1.23	General Service Company Correspondence	5		5			
1.2.005	1.24	Records Retention Schedule Agency Copy	US		US		Convenience Copy (11.00)	
1.2.008	1.245	Library Destruction Records	FE+3		FE+3			
3.1.036	1.25	Vocational Office Education Files	5		5		29 CFR 30.8(e)	
3.3.015	1.26	Position Questionnaires	US+3		US+3			
3.4.006	1.27	Employee Sign-in Sheet	FE+4		FE+4			

Retention Codes (Field 7)

AC – After Closed, Terminated, Completed, Expired, Settled
 AV – Administrative Value

CE – Calendar Year End
 FE – Fiscal Year End

LA – Life of Asset
 MO – Months

PM – Permanent
 US – Until Superseded

Archival Codes (Field 8)

A – Transfer to State Archives
 R – Review by State Archivist



STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 15 of 75

2. Agency Code 307		3. Agency Name Secretary of State							
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.
			Agency	Storage	Total				

3.4	1.28	Flex-Time Request	US+3		US+3				
3.3.020	1.29	Employee Vacation Schedules	1		1				
3.4.002	1.30	Monthly Leave Balance Sheet	FE+3		FE+3				
5.1.014	1.31	Time Sheet Procedures	US+1		US+1				
1.1.071	1.32	Background Material for Handbook	AC+3		AC+3		AC = Completion or termination of program, rules, policies, or procedures.		
3.4.007	1.33	Request for Leave Sheets	FE+3		FE+3				
4.7.003	1.34	Hot Checks	AC+3		AC+3		AC = After deemed uncollectable.		
4.7.003	1.345	Hot Checks/Insufficient Funds	AC+3		AC+3		AC = After deemed uncollectable.		
4.2.005	1.35	Central Supply Store Receipts	FE+5		FE+5				
4.7.011	1.355	Central Supply Store Balance Sheet	FE+5		FE+5				
4.5.002	1.36	Monthly Reports	FE+3		FE+3				
4.5.002	1.37	Weekly Reports	FE+3		FE+3				

Retention Codes (Field 7)

AC – After Closed, Terminated, Completed, Expired, Settled
AV – Administrative Value

CE – Calendar Year End
FE – Fiscal Year End

LA – Life of Asset
MO – Months

PM – Permanent
US – Until Superseded

Archival Codes (Field 8)

A – Transfer to State Archives
R – Review by State Archivist



STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 16 of 75

2. Agency Code 307		3. Agency Name Secretary of State							
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.
			Agency	Storage	Total				

4.5.002	1.38	Budget Reports	FE+3		FE+3				
4.5.002	1.40	Monthly Budget Reports	FE+3		FE+3				
1	1.41	Daily Inventory Records	FE+3		FE+3				
4.7	1.43	Revoked/Cancelled Filings	FE+3		FE+3				
4.7	1.44	Bankruptcy Notices	AC+1		AC+1	AC = Date of Filing.			
4.7	1.45	Reinstated Filings	FE+5		FE+5				
5.1.007	1.46	Print Requests	FE+1		FE+1				
1.1.008	1.47	Mail Outs Marketing	US+2		US+2				
5.2.008	1.48	Repair Requests	LA+5		LA+5	LA = Disposal of Equipment.			
5.2.020	1.49	Supply List	FE+1		FE+1				

Retention Codes (Field 7)

AC – After Closed, Terminated, Completed, Expired, Settled
 AV – Administrative Value

CE – Calendar Year End
 FE – Fiscal Year End

LA – Life of Asset
 MO – Months

PM – Permanent
 US – Until Superseded

Archival Codes (Field 8)

A – Transfer to State Archives
 R – Review by State Archivist



STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 17 of 75

2. Agency Code	307	3. Agency Name					Secretary of State				
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.		
			Agency	Storage	Total						

5.2.014	1.50	Equipment Inventory List	FE+3		FE+3				
5.2.003	1.51	Blueprints	LA		LA	R			
5.3.008	1.52	Purchase Requisitions	FE+5		FE+5				
5.4	1.54	Safety Memos	US+3		US+3				
5.5.002	1.55	Long Distance Phone Call Log	AC+ 1MO		AC+ 1MO		AC = Purpose Served.		
5.5.003	1.56	Management Telephone Reports	AC		AC		AC = End of Month.		
1.1.007	1.57	Development and Correspondence Concerning Utility Security Instruments	FE+5		FE+5	R			
1.1.063	1.58	Section Meeting Minutes	CE+2		CE+2				
1.1	1.60	Missing Checks Correspondence	FE+1		FE+1				

Retention Codes (Field 7)

AC – After Closed, Terminated, Completed, Expired, Settled
 AV – Administrative Value

CE – Calendar Year End
 FE – Fiscal Year End

LA – Life of Asset
 MO – Months

PM – Permanent
 US – Until Superseded

Archival Codes (Field 8)

A – Transfer to State Archives
 R – Review by State Archivist



STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 18 of 75

2. Agency Code		3. Agency Name		7. Retention Period		8. Archival		10.	11.
307		Secretary of State							TSLAC ONLY
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	Agency	Storage	Total	9. Remarks		106 No.	Amend. No.
1.1	1.9	Warrant Cancellation Requests	FE+5		FE+5				
1.1.008	2.01	Problem Filing Correspondence	CE+3		CE+3				
1.1.008	2.02	Duplicate Walker Number Correspondence	CE+3		CE+3				
1.1.008	2.025	Duplicate Number Correspondence	FE+5		FE+5				
1.1	2.04	Missing Attachments UCC I's	5 YRS.		5 YRS.				
5.1.014	2.05	Mail Procedures	US+3		US+3				
4.7	2.06	Unclaimed Acknowledgement Copies	60Days		60Days				
4.7	2.07	Fiscal Notes Request	AC+1		AC+1	AC = Cost Estimate Prepared.			

Retention Codes (Field 7)

AC – After Closed, Terminated, Completed, Expired, Settled
 AV – Administrative Value

CE – Calendar Year End
 FE – Fiscal Year End

LA – Life of Asset
 MO – Months

PM – Permanent
 US – Until Superseded

Archival Codes (Field 8)

A – Transfer to State Archives
 R – Review by State Archivist



STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 19 of 75

2. Agency Code 307		3. Agency Name Secretary of State							
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.
			Agency	Storage	Total				
4.7	2.08	Deleted Filing Records	FE+3		FE+3				
4.7	2.09	Backdated Filing Records	FE+3		FE+3				
4.7	2.10	Filing Number Limits	FE+5		FE+5				
4.7	3.01	Daily Reminder Books Data Entry	PM		PM				
1.1.069	3.02	Hourly Performance Rate	CE+2		CE+2				

Retention Codes (Field 7)

AC – After Closed, Terminated, Completed, Expired, Settled
 AV – Administrative Value

CE – Calendar Year End
 FE – Fiscal Year End

LA – Life of Asset
 MO – Months

PM – Permanent
 US – Until Superseded

Archival Codes (Field 8)

A – Transfer to State Archives
 R – Review by State Archivist



STATE OF TEXAS Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 20 of 75

2. Agency Code 307		3. Agency Name Secretary of State							
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.
			Agency	Storage	Total				

1.2.013	4.03	UCC Alpha Index Master File	PM	PM	PM	Microfiche master files for UCC documents.	08-307-247	
1	4.035	Master File Update	PM	PM	PM	Master at SRC. Dup. at agency.	94-307-193	

Retention Codes (Field 7)

AC – After Closed, Terminated, Completed, Expired, Settled
AV – Administrative Value

CE – Calendar Year End
FE – Fiscal Year End

LA – Life of Asset
MO – Months

PM – Permanent
US – Until Superseded

Archival Codes (Field 8)

A – Transfer to State Archives
R – Review by State Archivist



STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 21 of 75

2. Agency Code 307		3. Agency Name Secretary of State							
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.
			Agency	Storage	Total				
1	4.05	UCC Index Card Files	PM	PM	PM	Master at SRC. Dup. at agency.	94-307-199		
2.2.012	4.07	Amendment Number Cross Reference with Register No.	PM		PM				
2.2.012	4.08	Purge List NUC962RP/ID:NUC962PR	PM		PM				
5.1	5.01	Reader Printer Copy Count	6MO		6MO				
4.5.002	5.02	Reader Printer Tape Check Record	FE+5		FE+5				

Retention Codes (Field 7)

AC – After Closed, Terminated, Completed, Expired, Settled
AV – Administrative Value

CE – Calendar Year End
FE – Fiscal Year End

LA – Life of Asset
MO – Months

PM – Permanent
US – Until Superseded

Archival Codes (Field 8)

A – Transfer to State Archives
R – Review by State Archivist



STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 22 of 75

2. Agency Code 307		3. Agency Name Secretary of State							
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.
			Agency	Storage	Total				
4.7	5.03	Refund Authorizations	6MO		6MO				
4.7	5.04	UCC I Filings Financing Statements, Security Agreements, Federal Tax Liens, and Utility Security Instruments	6MO	2YR+ 6MO	3		Filmed at SRC, returned to agency for 6MO, stored at SRC for 2Y 6MO, then destroyed.	90-307-003	
4.7	5.04-M	UCC I Filings Financing Statements, Security Agreements, Federal Tax Liens, and Utility Security Instruments	PM	PM	PM		Master at SRC. Dup. at agency.	90-307-032	
4.7	5.05	Financing Statement Changes (UCC III's) Financing Statement Changes, Federal Tax Lien Releases, and Utility Security Instrument Supplements	6MO	2YR+ 6MO	3		Filmed at SRC, returned to agency for 6MO, stored at SRC for 2Y 6MO, then destroyed.	90-307-004	
4.7	5.05-M	Financing Statement Changes (UCC-III's) Financing Statement Changes, Federal Tax Lien Releases, and Utility Security Instrument Supplements	PM	PM	PM		Master at SRC. Dup. at agency.	90-307-033	

Retention Codes (Field 7)

AC – After Closed, Terminated, Completed, Expired, Settled
AV – Administrative Value

CE – Calendar Year End
FE – Fiscal Year End

LA – Life of Asset
MO – Months

PM – Permanent
US – Until Superseded

Archival Codes (Field 8)

A – Transfer to State Archives
R – Review by State Archivist



STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 23 of 75

2. Agency Code	307	3. Agency Name		Secretary of State					
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.
			Agency	Storage	Total				

1	5.055	Financing Statement & Security Agreement Attachment Files	PM	PM	PM	Master at SRC. Dup. at agency.	94-307-197	
4.7	5.065	Daily Reminder Books File Section	1YR+ 6MO		1YR+ 6MO			
1	5.066	Financing Statement & Security Agreement Oversize Files	PM	PM	PM	Master at SRC. Dup. at agency.	94-307-198	
4.7	5.07	Financing Statement & Security Agreements UCC I's	PM		PM	All filings prior to 1976.		
4.7	5.08	Financing Statement Changes UCC III's	PM		PM	All filings prior to 1976.		
4.7	5.09	Oversize Files	PM		PM	All filings prior to 1976.		
4.7	5.10	Attachment Files	PM		PM	All filings prior to 1976.		

Retention Codes (Field 7)

AC – After Closed, Terminated, Completed, Expired, Settled
 AV – Administrative Value

CE – Calendar Year End
 FE – Fiscal Year End

LA – Life of Asset
 MO – Months

PM – Permanent
 US – Until Superseded

Archival Codes (Field 8)

A – Transfer to State Archives
 R – Review by State Archivist



STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 24 of 75

2. Agency Code 307		3. Agency Name Secretary of State							
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.
			Agency	Storage	Total				

4.7	5.11	Utility Security Instruments USI	PM		PM	All filings prior to 1976.		
4.7	5.12	Utility Security Instrument (USI) Amendments	PM		PM	All filings prior to 1976.		
4.7	5.13	Federal Tax Lines FTL	PM		PM	All filings prior to 1976.		
4.7	5.14	Termination and Federal Tax Lien (FTL) Releases	PM		PM	All filings prior to 1976.		
4.7	5.15	Index Files	PM		PM	All filings prior to 1976.		
4.7	5.16	UCC Filings Financing Statements, Security Agreements, Notice of Federal Tax Liens, Utility Security Instruments, Financing Statement Amendments, Release of Federal Tax Liens, and Utility Security Instruments Supplements.	6MO	2YR+ 6MO	3		02-307-230	

Retention Codes (Field 7)

AC – After Closed, Terminated, Completed, Expired, Settled
AV – Administrative Value

CE – Calendar Year End
FE – Fiscal Year End

LA – Life of Asset
MO – Months

PM – Permanent
US – Until Superseded

Archival Codes (Field 8)

A – Transfer to State Archives
R – Review by State Archivist



STATE OF TEXAS Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 25 of 75

2. Agency Code 307		3. Agency Name Secretary of State								
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.	
			Agency	Storage	Total					

4.7	6.02	Expedite Search Requests	AC+ 3MO		AC+ 3MO	AC = After Paid.		
5.1.015	6.06	Federal Express Information Processed and Mailed out	1YR		1YR			
5.5	6.07	Fax Requests	AC+ 3MO		AC+ 3MO	AC = Verification of Billing.		

Retention Codes (Field 7)				Archival Codes (Field 8)	
AC – After Closed, Terminated, Completed, Expired, Settled	CE – Calendar Year End	LA – Life of Asset	PM – Permanent	A – Transfer to State Archives	
AV – Administrative Value	FE – Fiscal Year End	MO – Months	US – Until Superseded	R – Review by State Archivist	



STATE OF TEXAS Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 26 of 75

2. Agency Code 307		3. Agency Name Secretary of State							
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.
			Agency	Storage	Total				
5.5.002	6.09	Fax Transmission Reports	AC+ 6MO		AC+ 6MO	AC = Verification of Billing.			
5.5.002	6.10	Fax Copy Count	AC+ 1MO		AC+ 1MO	AC = End of Month.			
5.5.002	6.13	Fax Phone Log	AC+ 1MO		AC+ 1MO	AC = End of Month.			

Retention Codes (Field 7)

AC – After Closed, Terminated, Completed, Expired, Settled
AV – Administrative Value

CE – Calendar Year End
FE – Fiscal Year End

LA – Life of Asset
MO – Months

PM – Permanent
US – Until Superseded

Archival Codes (Field 8)

A – Transfer to State Archives
R – Review by State Archivist



STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 27 of 75

2. Agency Code 307		3. Agency Name Secretary of State						
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival 9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.
			Agency	Storage	Total			

1.1.002	7.01	Audit Letter/Reports	AC+7		AC+7	AC = Publication or release of final audit findings.		
1.1	7.02	Request for Refund	6MO		6MO			
1.1.008	7.03	Check Copy Request	AC+2		AC+2	AC = Fiscal Year End.		
4.1.007	7.04	Transfer of Funds to and from Account Numbers	FE+3		FE+3			
4.2.001	7.06	Deposit Vouchers	FE+5		FE+5			
4.2.001	7.08	Deposits	FE+10		FE+10			
4.2.005	7.09	State Purchase Vouchers	FE+3		FE+3			

Retention Codes (Field 7)	Archival Codes (Field 8)
AC – After Closed, Terminated, Completed, Expired, Settled AV – Administrative Value	A – Transfer to State Archives R – Review by State Archivist
CE – Calendar Year End FE – Fiscal Year End	PM – Permanent US – Until Superseded
LA – Life of Asset MO – Months	



STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 28 of 75

2. Agency Code 307		3. Agency Name Secretary of State							
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.
			Agency	Storage	Total				

4.7	7.11	6.	7. Agency	7. Storage	7. Total	8.	9.	10.	11.
		Register Number Records	PM		PM				
4.2.001	7.13	Legal Ease	1	5	6			98-307-216	
4.2.001	7.14	Credit Cards	1	5	6			98-307-217	
4.2.001	7.15	Packing Slips	FE	3	FE+3			04-307-232	
4.2.001	7.16	Client Account	1	5	6			07-307-238	

Retention Codes (Field 7)

AC – After Closed, Terminated, Completed, Expired, Settled
 AV – Administrative Value

CE – Calendar Year End
 FE – Fiscal Year End

LA – Life of Asset
 MO – Months

PM – Permanent
 US – Until Superseded

Archival Codes (Field 8)

A – Transfer to State Archives
 R – Review by State Archivist



STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 29 of 75

2. Agency Code 307		3. Agency Name Secretary of State							
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.
			Agency	Storage	Total				

1	3	Religious Congregation Trustees	PM		PM				
3.4.007	10.05	Time Off and/or Sick Leave Requests	FE+3		FE+3				
1.1.014	10.10	Legal Opinions and Advice From agency legal counsel or the Attorney General, including any requests eliciting the opinions.	AV		AV	R			
1.1.063	10.30	Meeting Minutes/Notes – Staff Minutes and notes of internal staff meetings.	1		1				
5.5.002	10.40	Long Distance Telephone Log	AV		AV				
1.1.027	10.50	Proposed Legislation	AV		AV				

Retention Codes (Field 7)

AC – After Closed, Terminated, Completed, Expired, Settled
AV – Administrative Value

CE – Calendar Year End
FE – Fiscal Year End

LA – Life of Asset
MO – Months

PM – Permanent
US – Until Superseded

Archival Codes (Field 8)

A – Transfer to State Archives
R – Review by State Archivist



STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 30 of 75

2. Agency Code 307		3. Agency Name Secretary of State								
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.	
			Agency	Storage	Total					
1.1.069	10.60	Monthly Reports	1		1					
1.2.006	10.80	Records Transmittal Forms	AC+2		AC+2		AC = disposition of records.			
1.2.008	10.90	Request for Authority to Dispose of State Records (RMD 102)	FE+3		FE+3					
1.2.005	11.00	Records Retention Schedule Agency copy	US		US					
1.2.012	11.10	Records Inventory Worksheets	US		US					
5.2.008	11.20	Equipment History File; Equipment Service Agreements	LA+3		LA+3					
1	11.40	Athlete Agents	2	20	22			93-307-184		
1	11.45	Athlete Agent Preliminary Reports	3	17	20			08-307-242		
3.1.035	11.50	3 rd Party Debt Collectors/Credit Bureau Bonds	AC+3	7	AC+10		AC = Bonds have expired, cancelled.	02-307-229		

Retention Codes (Field 7)

AC – After Closed, Terminated, Completed, Expired, Settled
 AV – Administrative Value

CE – Calendar Year End
 FE – Fiscal Year End

LA – Life of Asset
 MO – Months

PM – Permanent
 US – Until Superseded

Archival Codes (Field 8)

A – Transfer to State Archives
 R – Review by State Archivist



STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 31 of 75

2. Agency Code 307		3. Agency Name Secretary of State							
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.
			Agency	Storage	Total				

1	11.60	Business Opportunity Filings	2	4	6	Paper retained for 2 years then sent to SRC for filming, paper kept at SRC for remainder of retention, then destroyed. Master at SRC. Dup. at agency. State Records Center (SRC) AC=Date of Microfilming/Master SRC Dup.at agency.AC= Date of Microfilming. Paper retained for 2 MO then filmed at SRC. Paper returned to agency, then destroyed. AC=Date of Microfilming. Master at SRC Dup. at agency.AC=Date of Microfilming. Master at SRC	90-307-024	
1	11.60-M	Business Opportunity Filings	PM	PM	PM		91-307-088	
1	11.70	Business Opportunity Complaints	1MO	4 YR+ 11MO	5		93-307-186	
1	11.80	Membership Camping Resorts	1	20	21		93-307-185	
1	11.90-E	Citations - Other	PM		PM			
1	11.90-M1	Citations – Other (Master)	0	AC+100	AC+100		92-307-123	
1	11.90-M2	Citations – Other (Dup.)	AC+100		AC+100			
1	11.95-1	Citations (Master)	0	AC+100	AC+100		98-307-221	
1	11.95-2	Citations (Dup.)	AC+100		AC+100			
Retention Codes (Field 7)							Archival Codes (Field 10)	

AC – After Closed, Terminated, Completed, Expired, Settled
 AV – Administrative Value
 CE – Calendar Year End
 FE – Fiscal Year End
 LA – Life of Asset
 MO – Months
 PM – Permanent
 US – Until Superseded
 A – Transfer to State Archives
 R – Review by State Archivist





STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 32 of 75

2. Agency Code 307		3. Agency Name Secretary of State							
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.
			Agency	Storage	Total				

1	11-95-E	Citations	PM		PM	Electronic records maintained as long as microfilm version is kept.			
1	12.00-M1	Citations – Texas (Master)	0	AC+100	AC+100	AC=Date of Microfilming/Master at SRC.	92-307-120		
1	12.00-M2	Citations – Texas (Dup.)	AC+100		AC+100	Dup.at agency. AC=Date of Microfilming/Master at SRC.			
1	12.10-M1	Citations – Special Suits (Master)	0	AC+100	AC+100	AC=Date of Microfilming/Master at SRC.	92-307-121		
1	12.10-M2	Citations – Special Suits (Dup.)	AC+100		AC+100	Dup. at agency. AC=Date of Microfilming/Master at SRC.			
Retention Codes (Field 7)							Archival Codes (Field 8)		

AC – After Closed, Terminated, Completed, Expired, Settled
AV – Administrative Value

CE – Calendar Year End
FE – Fiscal Year End

LA – Life of Asset
MO – Months

PM – Permanent
US – Until Superseded

A – Transfer to State Archives
R – Review by State Archivist



STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 33 of 75

2. Agency Code 307		3. Agency Name Secretary of State							
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.
			Agency	Storage	Total				

1	12.20-1	Citations – Misc. (Master)	0	AC+100	AC+100	Paper retained for 1 year then filmed at SRC. Paper returned to agency, then destroyed. AC=Date of Microfilming Master at SRC.	92-307-122	
1	12.20-2	Citations – Misc. (Dup.)	AC+100		AC+100	Dup.at agency. AC=Date of Microfilming Master at SRC.	98-307-223	
1	12.25-M1	Citations – Comptroller (Master)	0	AC+100	AC+100	Electronic records maintained as long as microfilm version is kept. AC=Date of Microfilming Master at SRC.		
1	12.25-M2	Citations – Comptroller (Dup.)	AC+100		AC+100	Dup.at agency. AC=Date of Microfilming Master at SRC.		

Retention Codes (Field 7)

Archival Codes (Field 8)

AC – After Closed, Terminated, Completed, Expired, Settled
AV – Administrative Value

CE – Calendar Year End
FE – Fiscal Year End

LA – Life of Asset
MO – Months

PM – Permanent
US – Until Superseded

A – Transfer to State Archives
R – Review by State Archivist



STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 34 of 75

2. Agency Code 307		3. Agency Name Secretary of State								
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.	
			Agency	Storage	Total					
1.2.013	12.30	Citation Index Cards	PM	PM	PM		Master at SRC. Dup. at agency.	92-307-124		
5.1.003	12.40	Certified/Registered Mail Lists	2		2					
1	12.60	Texas Alcoholic Beverage Code Notice of Hearings and Orders	2		2					
1	12.70-E	Returned Process Citations	AC+100		AC+100		AC = Date of Implementation of New Citations System. (11-25-1996)			
1.2	12.80	Yellow Pads with Money Numbers & Reference Numbers Citations Logs	3	7	10			93-307-190		

Retention Codes (Field 7)

AC – After Closed, Terminated, Completed, Expired, Settled
 AV – Administrative Value

CE – Calendar Year End
 FE – Fiscal Year End

LA – Life of Asset
 MO – Months

PM – Permanent
 US – Until Superseded

Archival Codes (Field 8)

A – Transfer to State Archives
 R – Review by State Archivist



STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 35 of 75

2. Agency Code 307		3. Agency Name Secretary of State							
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.
			Agency	Storage	Total				

1	12.90	City Charter Home Rule City Charters & Amendments, Charter Amendments if incorporated by Republic of Texas or Acts of Legislature, Consolidations, Municipal Parking Authorities.	4		4	A	Paper filmed at SRC, paper returned to agency until agency retention period is met, then paper transferred to Archives.		
1	12-90-M	City Charter Home Rule City Charters & Amendments, Charter Amendments if incorporated by Republic of Texas or Acts of Legislature, Consolidations, Municipal Parking Authorities.	PM	PM	PM		Master at SRC. Dup. at agency.	92-307-125	

Retention Codes (Field 7)

AC – After Closed, Terminated, Completed, Expired, Settled
AV – Administrative Value

CE – Calendar Year End
FE – Fiscal Year End

LA – Life of Asset
MO – Months

PM – Permanent
US – Until Superseded

Archival Codes (Field 8)

A – Transfer to State Archives
R – Review by State Archivist



STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 36 of 75

2. Agency Code 307		3. Agency Name Secretary of State								
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	10. 106 No.	11. TSLAC ONLY Amend. No.		
			Agency	Storage	Total				9. Remarks	
1	13.00	Governor's Official Commissions	AC		AC	Paper filmed at SRC at the end of a governor's term of office, paper returned to agency, then paper destroyed. AC = End of governor's term of office.				
1	13.00-E	Governor's Official Commissions	PM		PM					
1	13.00-M1	Governor's Official Commissions (Master) Microfilm Titles: Boards & Commissions, Appellate Courts, Court of Appeals, Chief Elected Officials, Judges of the Adm. Judicial Regions, Texas Judicial Council, Commissioner of Deeds, Commissioner of Appeals of the Supreme Court, District Judges, Criminal District Judges, District Attorneys, Criminal District Attorneys, Special County Judges	0	AC+100	AC+100	AC = End of governor's term of office Master at SRC.	92-307-126			
1	13.00-M2	Governor's Official Commissions (Dup.)	AC+100		AC+100	Dup. at agency. AC=End of governor's term of office.				

Retention Codes (Field 7)				Archival Codes (Field 8)	
AC – After Closed, Terminated, Completed, Expired, Settled	CE – Calendar Year End	LA – Life of Asset	PM – Permanent	A – Transfer to State Archives	
AV – Administrative Value	FE – Fiscal Year End	MO – Months	US – Until Superseded	R – Review by State Archivist	



STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 37 of 75

2. Agency Code 307		3. Agency Name Secretary of State							
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.
			Agency	Storage	Total				

1.1.008	13.10	Correspondence, General Miscellaneous and Office	2		2				
1	13.20	Credit Services Organizations	1	9	10			08-307-241	
1	13.30	Election Registers aka Appointment Registers	10		10	A			
1	13.50	Health Spas	AC+ 1MO		AC+ 1MO		Paper filmed at SRC after the file has been closed, paper returned to agency, then paper destroyed. AC = After file is closed.		
1	13.50-M	Health Spas	PM	PM	PM		Master at SRC. Dup. at agency.	94-307-204	

Retention Codes (Field 7)

AC – After Closed, Terminated, Completed, Expired, Settled
AV – Administrative Value

CE – Calendar Year End
FE – Fiscal Year End

LA – Life of Asset
MO – Months

PM – Permanent
US – Until Superseded

Archival Codes (Field 8)

A – Transfer to State Archives
R – Review by State Archivist



STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 38 of 75

2. Agency Code 307		3. Agency Name Secretary of State							
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.
			Agency	Storage	Total				

1	13.60	Legislative Bills and Resolutions Filed	AC		AC	A	AC=Paper originals sent to contract vendor for scanning, returned to SOS. Paper originals then sent to contract vendor for binding and transferred to archives.		
1	13.60-E	Legislative Bills and Resolutions Filed – Electronic copies	2		2	A	Electronic files maintained on SOS servers for public access for one additional session-then removed to University of North Texas archives for permanent retention.		
1	13.60-M	Legislative Bills and Resolutions Filed – General and Special Laws	0	PM		PM	Gov Code §2158.064 stating this requirement was repealed by 82 nd Legislature, First Called Special Session.	92-307-132	

Retention Codes (Field 7)	Archival Codes (Field 8)
AC – After Closed, Terminated, Completed, Expired, Settled AV – Administrative Value CE – Calendar Year End FE – Fiscal Year End LA – Life of Asset MO – Months PM – Permanent US – Until Superseded	A – Transfer to State Archives R – Review by State Archivist



STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 39 of 75

2. Agency Code	307	3. Agency Name					Secretary of State				
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.		
			Agency	Storage	Total						

1	13.70	Liquor Power of Attorneys	2		2	Paper retained for 2 years then filmed at SRC. Paper returned to agency, then destroyed. Electronic records maintained as long as microfilm version is kept.		
1	13.70-M1	Liquor Power of Attorneys (Master)	0	AC+100	AC+100	AC=Date of Microfilming/Master SRC	92-307-140	
1	13.70-M2	Liquor Power of Attorneys (Dup.)	AC+100		AC+100	Dup. at agency. AC=Date of Microfilming/Master SRC.	91-307-061	
4	13.90	Money Records	6 MO	3 YR+ 6 MO	4		98-307-218	
4	13.95	Money Records Credit Card Payments	FE	3	FE+3		91-307-069	
1	14.00	Municipal Boundary Listings	1	2	3			

Retention Codes (Field 7)

AC – After Closed, Terminated, Completed, Expired, Settled
AV – Administrative Value

CE – Calendar Year End
FE – Fiscal Year End

LA – Life of Asset
MO – Months

PM – Permanent
US – Until Superseded

Archival Codes (Field 8)

A – Transfer to State Archives
R – Review by State Archivist



STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 40 of 75

2. Agency Code 307		3. Agency Name Secretary of State							
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.
			Agency	Storage	Total				

4	14.10	Money Records on Notary Public Certifications	6MO	3YR+ 6 MO	4			92-307-152	
4.2.002	14.20	Money Receipt Books	FE+3		FE+3				
1	14.30	Notary Applications	3MO	5YR+ 9MO	6		Paper sent to SRC for filming, paper kept at SRC for remainder of retention, then destroyed.	90-307-007	
1	14.30-E	Notary Applications	PM		PM				
1	14.30-M1	Notary Applications (Master)	0	60	60		Master at SRC.	92-307-173	
1	14.30-M2	Notary Applications (Dup.)	60	0	60		Dup. at agency.	90-307-013	
1	14.35	Notary Public Applications Final Rejections	90 DAYS		90 DAYS		AC= File is Closed.		
1	14.40	Notary Public Bonds	3MO	5YR+ 9MO	6		Paper sent to SRC for filming, paper kept at SRC for remainder of retention, then destroyed.		

Retention Codes (Field 7)

AC – After Closed, Terminated, Completed, Expired, Settled
AV – Administrative Value

CE – Calendar Year End
FE – Fiscal Year End

LA – Life of Asset
MO – Months

PM – Permanent
US – Until Superseded

Archival Codes (Field 8)

A – Transfer to State Archives
R – Review by State Archivist





STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 41 of 75

2. Agency Code 307		3. Agency Name Secretary of State							
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.
			Agency	Storage	Total				

1	14.40-E	Notary Public Bonds	PM		PM				
1.1	14.40-M1	Notary Public Bonds (Master)	0	60	60		Master at SRC.	92-307-171	
1.1	14.40-M2	Notary Public Bonds (Dup.)	60		60		Dup. at agency.		
1	14.50	Notary Public Complaints	AC+1	9	AC+10		AC = File is closed.	00-307-228	
1	14.60	Notary Public Applications w/Convictions	AC	4	AC+4		AC = File is closed.	08-307-243	
1	14.65	Notary Public Educational Video	US		US		US = until replaced or becomes obsolete. Copies to Texas State Publications Depository Program.		
1	14.70	Notary Files	PM	PM	PM			92-307-136	
1	14.80	Notary Public Appointment & Reappointments	PM	PM	PM			90-307-055	
1	14.85	Notary Public Address Changes	3 MO		3 MO				
1	14.90	Official List of Notaries Public	8		8	A	Bound Volumes.		

Retention Codes (Field 7)

AC – After Closed, Terminated, Completed, Expired, Settled
 AV – Administrative Value

CE – Calendar Year End
 FE – Fiscal Year End

LA – Life of Asset
 MO – Months

PM – Permanent
 US – Until Superseded

Archival Codes (Field 8)

A – Transfer to State Archives
 R – Review by State Archivist



STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 42 of 75

2. Agency Code 307		3. Agency Name Secretary of State								
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.	
			Agency	Storage	Total					

1	15.00	Notary Public Reference Files	10		10		Discontinue Microfilming.		
1	15.00-M1	Notary Public Reference Files (Master)	0	AC+50	AC+50		AC=Date of Microfilming Master SRC	92-307-137	
1	15.00-M2	Notary Public Reference Files (Dup.)	AC+50		AC+50		Dup. at agency. AC=Date of Microfilming Master at SRC.		
1	15.10	Notary Public Cleared Suspense	1	5	6		Paper maintained for 1 year, then sent to SRC for filming, kept at SRC for remainder of retention period, then destroyed.	92-307-162	
1	15.10-E	Notary Public Cleared Suspense	PM		PM				
1	15.10-M1	Notary Public Cleared Suspense (Master)	0	60	60		Master at SRC.	92-307-163	
1	15.10-M2	Notary Public Cleared Suspense (Dup.)	60		60		Dup. at agency.		
1	15.11	List of US states & territories that require a Notary Public to attach seal.	US		US				

Retention Codes (Field 7)

AC – After Closed, Terminated, Completed, Expired, Settled
 AV – Administrative Value

CE – Calendar Year End
 FE – Fiscal Year End

LA – Life of Asset
 MO – Months

PM – Permanent
 US – Until Superseded

Archival Codes (Field 8)

A – Transfer to State Archives
 R – Review by State Archivist



STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 43 of 75

2. Agency Code 307		3. Agency Name Secretary of State								
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.	
			Agency	Storage	Total					

1	15.20	Governor's Clemency Proclamations	1		1	A			
1.2.013	15.30	Governor's Proclamations Alphabetical Card Index	PM		PM				
1.2.013	15.30-M	Governor's Proclamations Alphabetical Card Index	PM	PM	PM		Master at SRC. Dup. at agency.	92-307-130	
1	15.40	Property Rights for claim for the use of a deceased individual's name, voice, etc.	AC+50		AC+50		AC = After Death Tex. Prop. Code Ann. §26.006		
1	15.50	Public Safety Organizations	2	8	10			07-307-233	
1	15.60	Public Safety Solicitors	2	8	10			07-307-234	
1	15.70	Public Safety Solicitors Bond	AC+5		AC+5		AC = Bonds have expired, cancelled.		

Retention Codes (Field 7)

AC – After Closed, Terminated, Completed, Expired, Settled
 AV – Administrative Value

CE – Calendar Year End
 FE – Fiscal Year End

LA – Life of Asset
 MO – Months

PM – Permanent
 US – Until Superseded

Archival Codes (Field 8)

A – Transfer to State Archives
 R – Review by State Archivist



STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 44 of 75

2. Agency Code 307		3. Agency Name Secretary of State								
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.	
			Agency	Storage	Total					

1	15.80	Railroad Filings Railroad Charters	10	PM	PM	10	A	Master at SRC. Dup. at agency.	92-307-145	A1
1	15.80-M	Railroad Filings Railroad Charters	PM	PM	PM					
1.2.013	15.90	Railroad Index Cards	PM		PM					
1.2.013	15.90-M	Railroad Index Cards	PM	PM	PM			Master at SRC. Dup. at agency.	92-307-146	
1	16.00	Licensing of commercial use of State Seal of Texas	1	5	6				08-307-239	
1.3.001	16.10	Session Laws aka General & Special Laws of Texas	AC+7		AC+7			Bound Volumes. AC = Date of Publication Copies to Texas State Publications Depository Program, TSLAC.		

Retention Codes (Field 7)	Archival Codes (Field 8)
AC – After Closed, Terminated, Completed, Expired, Settled AV – Administrative Value	A – Transfer to State Archives R – Review by State Archivist
CE – Calendar Year End FE – Fiscal Year End	LA – Life of Asset MO – Months
PM – Permanent US – Until Superseded	



STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 45 of 75

2. Agency Code	307	3. Agency Name Secretary of State						
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	10. 106 No.	11. TSLAC ONLY Amend. No.
			Agency	Storage	Total	9. Remarks		

1	16.40	Telephone Solicitors	2	8	10		07-307-235	
3.1.035	16.50	Telephone Solicitors Bond	AC+4		AC+4	AC = Bonds have expired, cancelled.		
1	16.55	Telephone Solicitation Claims	AC+5		AC+5	AC = After notice to claimants.		
1	16.60	Veterans Organizations	2	8	10		07-307-236	
1	16.70	Veterans Solicitors	2	8	10		07-307-237	
3.1.035	16.80	Veterans Solicitors Bond	AC+4		AC+4	AC = Bonds have expired, cancelled.		
1	16.90	Wrestling Promoters	1	5	6	Paper retained for 1 year then filmed at SCR. Paper kept at SCR for 5 years then destroyed. Repealed effective: Sept. 1, 2005	92-307-165	
1	16.90-M1	Wrestling Promoters (Master)	0	25	25	Repealed effective: Sept. 1, 2005 Master at SRC	98-307-222	
1	16.90-M2	Wrestling Promoters (Dup.)	25		25	Dup. at agency.		

Retention Codes (Field 7)

AC – After Closed, Terminated, Completed, Expired, Settled
AV – Administrative Value

CE – Calendar Year End
FE – Fiscal Year End

LA – Life of Asset
MO – Months

PM – Permanent
US – Until Superseded

Archival Codes (Field 8)

A – Transfer to State Archives
R – Review by State Archivist



STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 46 of 75

2. Agency Code 307		3. Agency Name Secretary of State							
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.
			Agency	Storage	Total				

1.1.057	17.00	Transitory Information	AC		AC		Paper, Electronic or Voice Mail AC = Purpose of record has been fulfilled.		
1	17.10	Criminal History Reports	AV		AV				
1	24	Labor Union Reports	5		5	R	Paper sent to SRC for filming, paper returned to agency, film is checked, then paper destroyed. Electronic records maintained as long as microfilm version exists.		
1	24-M1	Labor Union Reports (Master)	0	AC+25	AC+25		AC=Date of Microfilming/Master SRC	92-307-139	
1	24-M2	Labor Union Reports (Dup.)	AC+25		AC+25		Dup.at agency. AC=Date of Microfilming/Master SRC.		
1	30	Labor Organizer Applications	5		5		Paper sent to SRC for filming, paper returned to agency, film is checked, then paper destroyed.		
1	30-M1	Labor Organizer Applications (Master)	0	AC+25	AC+25		AC=Date of Microfilming/Master SRC	92-307-138	
1	30-M2	Labor Organizer Applications (Dup.)	AC+25		AC+25		Dup.at agency.AC=(Same as above)		

Retention Codes (Field 7)

AC – After Closed, Terminated, Completed, Expired, Settled
AV – Administrative Value

CE – Calendar Year End
FE – Fiscal Year End

LA – Life of Asset
MO – Months

PM – Permanent
US – Until Superseded

Archival Codes (Field 8)

A – Transfer to State Archives
R – Review by State Archivist



STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 47 of 75

2. Agency Code 307		3. Agency Name Secretary of State								
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.	
			Agency	Storage	Total					
1	41	Governor's Official Proclamations	10		10	A	Discontinue Microfilming.			
1	41-M1	Governor's Official Proclamations (Master)	0	AC+100	AC+100		AC=Date of Microfilming Master at SRC. Last Date Microfilmed: 12/17/1991.	92-307-128		
1	41-M2	Governor's Official Proclamations (Dup.)	AC+100		AC+100		Dup. at agency. AC=Date of Microfilming Master at SRC.			
1	44	Organization of Soil Conservation Districts	10		10	R	Discontinue Microfilming.			
1	44-M1	Organization of Soil Conservation Districts (Master)	0	AC+10	AC+10		AC=Date of Microfilming Master at SRC. Last Date Microfilmed 10/7/1988.	92-307-149		
1	44-M2	Organization of Soil Conservation Districts (Dup.)	AC+10		AC+10		Dup. at agency. AC=Date of Microfilming Master at SRC.			
1.1.002	50	Audit Reports	AC+1	6	AC+7		Paper & Electronic. AC=Publication or release of final audit findings. Electronic records maintained as long as paper records are kept.	93-307-187		

Retention Codes (Field 7)

AC – After Closed, Terminated, Completed, Expired, Settled
AV – Administrative Value

CE – Calendar Year End
FE – Fiscal Year End

LA – Life of Asset
MO – Months

PM – Permanent
US – Until Superseded

Archival Codes (Field 8)

A – Transfer to State Archives
R – Review by State Archivist



STATE OF TEXAS Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 48 of 75

2. Agency Code 307		3. Agency Name Secretary of State							
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.
			Agency	Storage	Total				
1	63	Deeds of Cession	10		10	A			
1	75	Supreme Court Rules and Amendments	10		10	A			
1	75-E	Supreme Court Rules and Amendments	PM		PM	Electronic records maintained permanently.			
1	97	Miscellaneous Filings Not Statutorily Required	6MO		6MO				
1	118	River Compacts	10		10		A		

Retention Codes (Field 7)				Archival Codes (Field 8)	
AC – After Closed, Terminated, Completed, Expired, Settled	CE – Calendar Year End	LA – Life of Asset	PM – Permanent	A – Transfer to State Archives	
AV – Administrative Value	FE – Fiscal Year End	MO – Months	US – Until Superseded	R – Review by State Archivist	



STATE OF TEXAS Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 49 of 75

2. Agency Code 307		3. Agency Name Secretary of State								
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.	
			Agency	Storage	Total					

1.1.011	121	Governor's Executive Orders	10		10	A	Discontinue Microfilming	92-307-127	
1.1.011	121-E	Governor's Executive Orders	PM		PM		AC=Date of Microfilming/Master SRC Last Date Microfilmed: Jan. 8, 1988		
1.1.011	121-M	Governor's Executive Orders (Master)		AC+100	AC+100				
1.1.011	121-D	Governor's Executive Orders (Dup.)	AC+100		AC+100		Dup.at agency. AC=Date of Microfilming/Master SRC. Last Date Microfilmed: Jan. 8, 1988		
1	122	Federal Census Reports	20		20				
1	124	Ratifying of U.S. Constitution	10		10	A			

Retention Codes (Field 7)	Archival Codes (Field 8)
AC – After Closed, Terminated, Completed, Expired, Settled AV – Administrative Value	A – Transfer to State Archives R – Review by State Archivist
CE – Calendar Year End FE – Fiscal Year End	PM – Permanent US – Until Superseded
LA – Life of Asset MO – Months	



STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 50 of 75

2. Agency Code 307		3. Agency Name Secretary of State								
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.	
			Agency	Storage	Total					

3.1.035	138	Employee Bonds Texas Hospital Equipment Financing Council, State Public Employees, State Librarian and the Records Presv. Officer	AC	10	AC+10	AC = Bonds have expired, cancelled Discontinue Microfilming	08-307-240	
3.1.035	138-M1	Employee Bonds (Master) Texas Hospital Equipment Financing Council, State Public Employees, State Librarian and the Records Presv. Officer	0	AC+10	AC+10	AC = Expiration of termination of the bond according to its terms Master at SRC.	92-307-118	
3.1.035	138-M2	Employee Bonds (Dup.)	AC+10		AC+10	Dup. at agency. AC = Expiration of termination of the bond according to its term.		
1	145	Copies of Other States Resolutions	20		20			
1	146	Auto Clubs & Salesman	1	9	10		93-307-188	

Retention Codes (Field 7)

AC – After Closed, Terminated, Completed, Expired, Settled
AV – Administrative Value

CE – Calendar Year End
FE – Fiscal Year End

LA – Life of Asset
MO – Months

PM – Permanent
US – Until Superseded

Archival Codes (Field 8)

A – Transfer to State Archives
R – Review by State Archivist



STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 51 of 75

2. Agency Code 307		3. Agency Name Secretary of State								
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival 9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.		
			Agency	Storage	Total					
3.1.035	149	Special District Bonds	AC+5		AC+5	Paper & Electronic AC = Bonds have expired, cancelled. Paper sent to SRC for filming, paper returned to agency, film checked, then paper destroyed. Electronic records maintained as long as paper records are kept.				
3.1.035	149-M1	Special District Bonds (Master)	0	AC+10	AC+10	AC = Bonds have expired or Cancelled. Master at SRC.	92-307-119			
3.1.035	149-M2	Special District Bonds (Dup.)	AC+10		AC+10	Dup. at agency. AC=Bonds have expired or Cancelled.	94-307-201			
1	152	Salary Supplements	1	19	20					
1	167	Authorization of Emergency Funds	10		10	A				

Retention Codes (Field 7)				Archival Codes (Field 8)			
AC – After Closed, Terminated, Completed, Expired, Settled	CE – Calendar Year End	LA – Life of Asset	PM – Permanent	A – Transfer to State Archives			
AV – Administrative Value	FE – Fiscal Year End	MO – Months	US – Until Superseded	R – Review by State Archivist			



STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 52 of 75

2. Agency Code 307		3. Agency Name Secretary of State							
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.
			Agency	Storage	Total				
1	170	Dissolution of Water Districts	PM		PM	R			
1	175	Controlled Substances Act	10		10				
1	183	Inaugural Fund	10		10	A			
1	184	County Owned & Operated Cemeteries	PM		PM				
1	186	Providing for the Purchase, Care, and Preservation of Alamo	10		10	A			

Retention Codes (Field 7)				Archival Codes (Field 8)	
AC – After Closed, Terminated, Completed, Expired, Settled	CE – Calendar Year End	LA – Life of Asset	PM – Permanent	A – Transfer to State Archives	R – Review by State Archivist
AV – Administrative Value	FE – Fiscal Year End	MO – Months	US – Until Superseded		



STATE OF TEXAS Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 53 of 75

2. Agency Code 307		3. Agency Name Secretary of State							
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.
			Agency	Storage	Total				

1	187	Apostilles	1		1	Discontinue Microfilming.		
1	187-E	Apostilles	PM		PM			
1	187-M	Apostilles	PM	PM	PM	Master at SRC. Dup. at agency.	91-307-065	
3.1.035	188	Invention Developer Bonds	AC+10		AC+10	AC=Bonds have expired or cancelled.		
1	189	Legislative Redistricting Board Plans Formerly File #123	10		10	A		

Retention Codes (Field 7)	Archival Codes (Field 8)
AC – After Closed, Terminated, Completed, Expired, Settled AV – Administrative Value	A – Transfer to State Archives R – Review by State Archivist
CE – Calendar Year End FE – Fiscal Year End	LA – Life of Asset MO – Months
PM – Permanent US – Until Superseded	



STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 54 of 75

2. Agency Code 307		3. Agency Name Secretary of State						
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	10. 106 No.	11. TSLAC ONLY Amend. No.
			Agency	Storage	Total			

1	193	Official Memorandum by the Secretary of State or Governor	10		10	A			
1	195	Firemen's Pension Plan Filings	10		10	R			
1	196	Emergency Interim Legislative Succession Act	US		US				
1	197	Interstate Mining Commission Bylaws and Amendments	20		20				

Retention Codes (Field 7)

AC – After Closed, Terminated, Completed, Expired, Settled
 AV – Administrative Value

CE – Calendar Year End
 FE – Fiscal Year End

LA – Life of Asset
 MO – Months

PM – Permanent
 US – Until Superseded

Archival Codes (Field 8)

A – Transfer to State Archives
 R – Review by State Archivist



STATE OF TEXAS Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 55 of 75

2. Agency Code 307		3. Agency Name Secretary of State								
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.	
			Agency	Storage	Total					

1	199	Authenticating Officer Governor Appointed	10		10	R			
1	201	Court of Appeals Rules and Amendments	10		10	A	Paper & Electronic Electronic records maintained permanently.		
1	202	Disclosure Statement of Conditional Gifts from foreign persons	10		10	R			
1	203	Cash Management Notes	10		10	A			

Retention Codes (Field 7)

AC – After Closed, Terminated, Completed, Expired, Settled
AV – Administrative Value

CE – Calendar Year End
FE – Fiscal Year End

LA – Life of Asset
MO – Months

PM – Permanent
US – Until Superseded

Archival Codes (Field 8)

A – Transfer to State Archives
R – Review by State Archivist





STATE OF TEXAS Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 56 of 75

2. Agency Code 307		3. Agency Name Secretary of State							
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.
			Agency	Storage	Total				
1	204	A list of endangered, threatened, or protected native plants	50		50	R			
1	205	Statement of Officer Bribery Statement	1	6	7			99-307-023	
1	205-E	Statement of Officer Bribery Statement	25		25				
1	206	Dissolved Districts	10		10				

Retention Codes (Field 7)				Archival Codes (Field 8)	
AC – After Closed, Terminated, Completed, Expired, Settled	CE – Calendar Year End	LA – Life of Asset	PM – Permanent	A – Transfer to State Archives	R – Review by State Archivist
AV – Administrative Value	FE – Fiscal Year End	MO – Months	US – Until Superseded		





STATE OF TEXAS Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 57 of 75

2. Agency Code 307		3. Agency Name Secretary of State							
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival		10. 106 No.	11. TSLAC ONLY Amend. No.
			Agency	Storage	Total	9. Remarks			
1	209	Declination of Remuneration	50		50				
1	210	Health/Human Services Trans./Train. Rpts.	10		10				
1	211	Groundwater Districts	10		10				
1	212	Water Districts/Non-Profit Water/Sewer Service Corps	10		10				
1	214	State Office of Administrative Hearings Closed Files	25		25				
1	218	Child Support Agreements Agreements with other countries for reciprocal treatment in child support cases (Official Acts of the Governor)	10		10	A			
1	222	Trans Texas Corridor Bonds	AC+10		AC+10		AC = After Expired or Cancelled.		

Retention Codes (Field 7)

AC – After Closed, Terminated, Completed, Expired, Settled
AV – Administrative Value

CE – Calendar Year End
FE – Fiscal Year End

LA – Life of Asset
MO – Months

PM – Permanent
US – Until Superseded

Archival Codes (Field 8)

A – Transfer to State Archives
R – Review by State Archivist





STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 58 of 75

2. Agency Code 307		3. Agency Name Secretary of State							
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.
			Agency	Storage	Total				
1	39	Game and Fish Proclamations Parks and Wildlife rules	PM	PM	PM		Master at SRC. Dup. at agency.	92-307-164	
1.1.008	50.00	Correspondence – General	2		2				
1	50.10	Attorney General Opinions and Requests for Opinions and Open Records Decisions	6MO		6MO		Contents published in TX. Register, original on file with Attorney General.		
1	50.10-M	Attorney General Opinions and Requests For Opinions and Open Records Decisions	20		20				
1	50.20-E	Notice of Open Meetings	PM		PM				
1	50.20-M1	Notice of Open Meetings (Master)	0	20	20		Master at SRC.	90-307-031	
1	50.20-M2	Notice of Open Meetings (Dup.)	20		20		Dup. at agency.		
1	50.25	Miscellaneous Documents/In Addition Notices	1		1		Microfilmed at SRC, paper destroyed.		
1	50.25-M	Miscellaneous Documents/In Addition Notices	PM		PM				

Retention Codes (Field 7)

AC – After Closed, Terminated, Completed, Expired, Settled
AV – Administrative Value

CE – Calendar Year End
FE – Fiscal Year End

LA – Life of Asset
MO – Months

PM – Permanent
US – Until Superseded

Archival Codes (Field 8)

A – Transfer to State Archives
R – Review by State Archivist



STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 59 of 75

2. Agency Code 307		3. Agency Name Secretary of State							
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.
			Agency	Storage	Total				

1.3.001	50.30	Bound volumes of Texas Register	PM		PM	§2002.001, Tex. Gov't Code requires all state agency rules to be indexed and published. Microfilmed by State Archives. Original copies in P.I. files (see below). Copies to Texas State Publications Depository Program, TSLAC.		
1.3.001	50.40	Bound volumes of Texas Administrative Code	PM		PM	Copies to Texas State Publications Depository Program, TSLAC.		
1	50.50	Texas Administrative Code	US		US	Computer database is exempt from Open Records Act (§2002.056, TX. Gov't Code).		
1	50.60	Original Public Inspection Files of all state agency rules published in the Texas Register	PM		PM	Working copies kept 3MO.		

Retention Codes (Field 7)

AC – After Closed, Terminated, Completed, Expired, Settled
AV – Administrative Value

CE – Calendar Year End
FE – Fiscal Year End

LA – Life of Asset
MO – Months

PM – Permanent
US – Until Superseded

Archival Codes (Field 8)

A – Transfer to State Archives
R – Review by State Archivist



STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 60 of 75

2. Agency Code 307		3. Agency Name Secretary of State							
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.
			Agency	Storage	Total				
1	50.60-M	Original Public Inspection Files of all state agency rules published in the Texas Register	PM	PM	PM		Master at SRC. Dup. at agency.	94-307-195	
1	50.70	Adoption by Reference Documents	PM		PM				
1	50.70-M	Adoption by Reference Documents	PM	PM	PM			91-307-089	

Retention Codes (Field 7)

AC – After Closed, Terminated, Completed, Expired, Settled
AV – Administrative Value

CE – Calendar Year End
FE – Fiscal Year End

LA – Life of Asset
MO – Months

PM – Permanent
US – Until Superseded

Archival Codes (Field 8)

A – Transfer to State Archives
R – Review by State Archivist



STATE OF TEXAS Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 61 of 75

2. Agency Code 307		3. Agency Name Secretary of State							
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.
			Agency	Storage	Total				
4.1.002	51.30	Subscription invoice and payment receipts	FE	3	FE+3			91-307-071	
1.1	51.40	Texas Register Working Copies	3MO		3MO				

Retention Codes (Field 7)

AC – After Closed, Terminated, Completed, Expired, Settled
AV – Administrative Value

CE – Calendar Year End
FE – Fiscal Year End

LA – Life of Asset
MO – Months

PM – Permanent
US – Until Superseded

Archival Codes (Field 8)

A – Transfer to State Archives
R – Review by State Archivist



STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 62 of 75

2. Agency Code 307		3. Agency Name Secretary of State							
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.
			Agency	Storage	Total				
1	1001	Corporations Documents	PM	PM	PM		Upon filing paper sent to SRC for filming, paper returned to agency and kept until corporation dissolved, forfeited or expired, then destroyed. Master at SRC. Dup. at agency.	90-307-036	
1	1003	Limited Partnership Doc.	PM		PM				
1	1004	Name Reservations	PM	PM	PM		Paper maintained 1 year, sent to SRC for filming, paper returned to agency, then destroyed. Master at SRC. Dup. at agency.	90-307-056	
1	1006	Name Registrations	PM	PM	PM		Paper maintained 1 year, sent to SRC for filming, paper returned to agency, then destroyed. Master at SRC. Dup. at agency.	94-307-194	
1	1008	Trademarks	PM	PM	PM		Upon filing paper sent to SRC for filming, returned to agency, then destroyed. Master at SRC. Dup. at agency.	90-307-057	

Retention Codes (Field 7)

AC – After Closed, Terminated, Completed, Expired, Settled
AV – Administrative Value

CE – Calendar Year End
FE – Fiscal Year End

LA – Life of Asset
MO – Months

PM – Permanent
US – Until Superseded

Archival Codes (Field 8)

A – Transfer to State Archives
R – Review by State Archivist



STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 63 of 75

2. Agency Code 307		3. Agency Name Secretary of State							
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.
			Agency	Storage	Total				

1	1010	Foreign Banks & Trusts	PM		PM	Upon filing paper sent to SRC for filming, returned to agency until dissolved, forfeited or expired, the destroyed.		
4.1	1012	Cert Bills	FE+1	2	FE+3		93-307-177	
4.2.005	1013	Paid Invoices	FE+1	2	FE+3		93-307-178	
1	1014	Walker Request/Receipts Work Orders	FE+1	2	FE+3		93-307-179	
1.1.008	1016	Correspondence - General	CE+2		CE+2			
1.1.008	1018	Information Letters	FE+1	2	FE+3		93-307-181	
1	1019	Suspense Records	3MO		3MO			

Retention Codes (Field 7)	Archival Codes (Field 8)
AC – After Closed, Terminated, Completed, Expired, Settled AV – Administrative Value	A – Transfer to State Archives R – Review by State Archivist
CE – Calendar Year End FE – Fiscal Year End	PM – Permanent US – Until Superseded
LA – Life of Asset MO – Months	





STATE OF TEXAS Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 64 of 75

2. Agency Code 307		3. Agency Name Secretary of State							
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.
			Agency	Storage	Total				

1.1.067	1020	Weekly Reports	CE+1	2	CE+3	AC = Until electronic records are transferred to and made usable in a new hardware or software environment with new documentation or there are no electronic records being retained to meet an approved retention period that require the documentation to be retrieved and read. 13 TAC 6.97(a)	93-307-182	
2.1.009	1021	Direct Access System Documentation	AC+3		AC+3			
2.2.002	1022	Direct Access Activity Records Utilization Reports	5		5			
2.2	1025	Computer Rewrite	AV		AV			

Retention Codes (Field 7)

AC – After Closed, Terminated, Completed, Expired, Settled
AV – Administrative Value

CE – Calendar Year End
FE – Fiscal Year End

LA – Life of Asset
MO – Months

PM – Permanent
US – Until Superseded

Archival Codes (Field 8)

A – Transfer to State Archives
R – Review by State Archivist



STATE OF TEXAS Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 65 of 75

2. Agency Code 307		3. Agency Name Secretary of State							
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.
			Agency	Storage	Total				

2.2.001	1026	Computer Printouts Activity Records	AV		AV			
5.5.004	1027	ACD Phone Reports	AV		AV	ACD = Automatic Call Distributor.		
5.1.003	1028	Certified Mail Receipt Books	1	FE+1	FE+2		93-307-191	
1	1029	Public Information Reports (PIR)	AV		AV			
1	1033	Imaged Corporation Documents	3MO	3	3Y+ 3MO		02-307-231	

Retention Codes (<i>Field 7</i>)	Archival Codes (<i>Field 8</i>)
AC – After Closed, Terminated, Completed, Expired, Settled AV – Administrative Value	A – Transfer to State Archives R – Review by State Archivist
CE – Calendar Year End FE – Fiscal Year End	LA – Life of Asset MO – Months
PM – Permanent	US – Until Superseded



STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 66 of 75

2. Agency Code 307		3. Agency Name Secretary of State								
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.	
			Agency	Storage	Total					

3.2	2000	Payroll Detail	CE+2	2	CE+4			08-307-245	
3.2.001	2001	Employee Deduction Authorizations	AC+2	2	AC+4	AC = After termination of employee or after amendment, expiration, or termination of authentication, whichever sooner.		08-307-246	
4.5.002	2002	Best End of Day Reports	FE	3	FE+3			90-307-046	
3.2.003	2004	Federal Tax Records	AC+4		AC+4	AC = Tax due date, date the claim is filed, or date tax is paid whichever is later. 26 CFR 31.6001 – 1(e)(2)			
3.2	2005	Direct Deposit Report	FE+1	2	FE+3			08-307-244	

Retention Codes (Field 7)

AC – After Closed, Terminated, Completed, Expired, Settled
 AV – Administrative Value

CE – Calendar Year End
 FE – Fiscal Year End

LA – Life of Asset
 MO – Months

PM – Permanent
 US – Until Superseded

Archival Codes (Field 8)

A – Transfer to State Archives
 R – Review by State Archivist



STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 67 of 75

2. Agency Code 307		3. Agency Name Secretary of State						
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival 9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.
			Agency	Storage	Total			

3.2.009	2007	Deferred Compensation/Texasaver	AC+5		AC+5	AC = distribution plan is complete.		
4.6.002	2008	Fixed Assets Reconciliation	FE	3	FE+3		91-307-075	
3.3.004	2009	Group Insurance Worksheet	US+1		US+1			
1.2.012	2010	Records Inventory Worksheets	US		US			
3.2.002	2011	Payroll Master	1	3	4		94-307-200	
5.2.014	2012	Inventory – Annual Physical	FE+3		FE+3			
4.7.009	2013	Fixed Asset Sequential Number Log	US+3		US+3			

Retention Codes (Field 7)

AC – After Closed, Terminated, Completed, Expired, Settled
 AV – Administrative Value

CE – Calendar Year End
 FE – Fiscal Year End

LA – Life of Asset
 MO – Months

PM – Permanent
 US – Until Superseded

Archival Codes (Field 8)

A – Transfer to State Archives
 R – Review by State Archivist



STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 68 of 75

2. Agency Code 307		3. Agency Name Secretary of State							
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.
			Agency	Storage	Total				

4.2.007	2014	Travel Vouchers Travel, payroll, etc.	FE	3	FE+3			90-307-039	
4.7.002	2015	Bank Statements	FE+3		FE+3				
4.2.005	2016	Purchase Order File	FE	3	FE+3			90-307-027	
4.2.005	2017	Purchase Voucher File	FE	3	FE+3			00-307-227	
4.2.005	2018	Cancelled Warrant Voucher	FE+3		FE+3				
4.2.001	2019	Cash Deposit Voucher/Detail	FE	3	FE+3			90-307-014	
4.2.003	2020	Revenue Refund Vouchers	FE	3	FE+3			90-307-015	
4.1.007	2023	Expenditure Transfers	FE+3		FE+3				
4.2.006	2024	General Journal Voucher – Comptroller	FE+3		FE+3				

Retention Codes (Field 7)

AC – After Closed, Terminated, Completed, Expired, Settled
 AV – Administrative Value

CE – Calendar Year End
 FE – Fiscal Year End

LA – Life of Asset
 MO – Months

PM – Permanent
 US – Until Superseded

Archival Codes (Field 8)

A – Transfer to State Archives
 R – Review by State Archivist



STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 69 of 75

2. Agency Code 307		3. Agency Name Secretary of State							
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.
			Agency	Storage	Total				

4.3.003	2025	Warrant Register DAFR 3651	FE+3		FE+3				
4.3	2026	Revenue/Receipts Transaction Register	FE+3		FE+3				
4.5.003	2027	Annual Financial Report	PM		PM		Copies to Texas State Publications Depository Program, TSLAC.		
4.5.001	2028	Audit Work Papers Annual Report	FE+3		FE+3	A			
1.1.002	2029	Reports – Audit from State Auditor’s	AC+7		AC+7			AC = Publication or release of final audit findings.	
4.5.002	2031	Security Filings with Treasury	FE+3		FE+3				

Retention Codes (Field 7)

AC – After Closed, Terminated, Completed, Expired, Settled
 AV – Administrative Value

CE – Calendar Year End
 FE – Fiscal Year End

LA – Life of Asset
 MO – Months

PM – Permanent
 US – Until Superseded

Archival Codes (Field 8)

A – Transfer to State Archives
 R – Review by State Archivist



STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 70 of 75

2. Agency Code 307		3. Agency Name Secretary of State							
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.
			Agency	Storage	Total				

4.4.003	2036	Fund Cash History Including Shared HAVA Funds	FE+3		FE+3				
4.4.002	2037	Accounts Receivable & Invoice Status	FE	3	FE+3			91-307-116	
4.7.003	2039	Non Sufficient Funds Checks from Treasury	AC+3		AC+3		AC = After deemed uncollectible.		
4.5.002	2041	Inaugural Fund	FE+3		FE+3				

Retention Codes (Field 7)	Archival Codes (Field 8)
AC – After Closed, Terminated, Completed, Expired, Settled AV – Administrative Value	A – Transfer to State Archives R – Review by State Archivist
CE – Calendar Year End FE – Fiscal Year End	PM – Permanent US – Until Superseded
LA – Life of Asset MO – Months	



STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 71 of 75

2. Agency Code 307		3. Agency Name Secretary of State								
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.	
			Agency	Storage	Total					

1.1.004	2042	Legislative Appropriations Request	AC+6		AC+6	A	AC = September 1 of odd-numbered calendar years. Copies to Texas State Publications Depository Program, TSLAC.		
1.1.004	2043	Instructions for Legislative Appropriations Request	US+6		US+6	R			
4.3.002	2045	Electronic Funds/Credit Card/Legalease & ACH	FE+3		FE+3				
4.2	2046	PCA Budget Revisions	FE+3		FE+3				
4.2	2047	Warrant Cancellations/Direct Deposit Reversals	FE+3		FE+3				

Retention Codes (Field 7)				Archival Codes (Field 8)			
AC – After Closed, Terminated, Completed, Expired, Settled	CE – Calendar Year End	LA – Life of Asset	PM – Permanent	A – Transfer to State Archives			
AV – Administrative Value	FE – Fiscal Year End	MO – Months	US – Until Superseded	R – Review by State Archivist			



STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 72 of 75

2. Agency Code 307		3. Agency Name Secretary of State						
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	10. 106 No.	11. TSLAC ONLY Amend. No.
			Agency	Storage	Total	9. Remarks		

1.1.002	2048	Internal Audit – Workpapers	AC+7		AC+7	AC = Publication or release of final audit findings.		
1.1.064	2049	Performance Measures File	FE+3		FE+3			
1.1.068	2050	Performance & Funds Management Report	AC+6		AC+6	AC = September 1 of odd-numbered calendar years. Copies to Texas State Publications Depository Program, TSLAC.		
1.1.055	2051	Strategic Plan	AC+6		AC+6	A AC = September 1 of odd-numbered calendar years. The archival requirement is met by sending the required copies of the plans to the Texas State Publications Depository Program, TSLAC.		

Retention Codes (Field 7)	Archival Codes (Field 8)
AC – After Closed, Terminated, Completed, Expired, Settled AV – Administrative Value	A – Transfer to State Archives R – Review by State Archivist
CE – Calendar Year End FE – Fiscal Year End	PM – Permanent US – Until Superseded
LA – Life of Asset MO – Months	





STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 73 of 75

2. Agency Code 307		3. Agency Name Secretary of State							
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.
			Agency	Storage	Total				

3.1	2600	Active Personnel Files	AC		AC	AC=After termination of employee Active Personnel Files become Terminated Personnel Files. AC=Terminated (Files will be retained for an additional 5 years).	93-307-176		
3.1	2601	Active Confidential Personnel Files	AC		AC				
3.1	2602	Disabled Employee Survey Sheets	FE+5		FE+5				
3.1	2603	New Employee Survey Sheet	FE+5		FE+5				
3.1	2604	Terminated Personnel Files	2	3	5				
3.4	2605	Cumulative Leave Status Report for Fiscal Year	FE+5		FE+5				
3.1.001	2606	Employment Applications – Not Hired	FE+2		FE+2				29 CFR 1602.31
3.1.014	2607	Employment Selections Records Job Closures	FE+5		FE+5				29 CFR 1602.31
3.1.019	2608	Performance Appraisals	2		2				29 CFR 1602.32(c)
3.1.023	2609	Position/Job Descriptions	AC+4		AC+4				40 TAC 815.106 (i); AC=Until Superseded or job eliminated.
3.1.029	2610	Employment Eligibility, Documentation or Verification of (INS 1-9)	AC+1		AC+1	AC=Termination of Employment. I-9s of employees who terminate before 3 yrs. Must be retained 3 yrs.			

Retention Codes (Field 7)

AC – After Closed, Terminated, Completed, Expired, Settled
AV – Administrative Value

CE – Calendar Year End
FE – Fiscal Year End

LA – Life of Asset
MO – Months

PM – Permanent
US – Until Superseded

Archival Codes (Field 8)

A – Transfer to State Archives
R – Review by State Archivist





STATE OF TEXAS

Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 74 of 75

2. Agency Code 307		3. Agency Name Secretary of State						
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	10. 106 No.	11. TSLAC ONLY Amend. No.
			Agency	Storage	Total	9. Remarks		

3.3.024	2619	Personnel Policies and Procedures Manual	US+3		US+3			
3.3.026	2620	Authorized Staffing Pattern	FE+5		FE+5	Replace within FE+2 so the FE+5 covers the retention period US+3		
3.3.026	2621	Quarterly FTE Reports to State Auditor	US+3		US+3			
3.3.026	2622	Staffing Forecast Report	FE+5		FE+5	Replace within FE+2 so the FE+5 covers the retention period US+3		
3.3.031	2623	EEO-4	3		3	29 CFR 1602.30,32,39,41,48,50		
3.3.031	2624	EEO-4 Federal Report	FE+5		FE+5	29 CFR 1602.30,32,39,41,48,50		
3.3.031	2625	EEO-4 Standardized Report	FE+5		FE+5	29 CFR 1602.30,32,39,41,48,50		
3.4.006	2626	Monthly Timesheets	FE+5		FE+5	40 TAC 815.106(i)		
3.4.006	2627	Monthly Time Reports	4		4	40 TAC 815.106(i)		
3.4.007	2628	Extended Sick Leave Requests	FE+5		FE+5			
3.4.007	2629	Family Medical Leave Documentation	FE+5		FE+5			

Retention Codes (Field 7)

Archival Codes (Field 8)

AC – After Closed, Terminated, Completed, Expired, Settled
AV – Administrative Value

CE – Calendar Year End
FE – Fiscal Year End

LA – Life of Asset
MO – Months

PM – Permanent
US – Until Superseded

A – Transfer to State Archives
R – Review by State Archivist



STATE OF TEXAS Records Retention Schedule

SLR 105

Form SLR 105C must accompany this form.

1. Page 75 of 75

2. Agency Code 307		3. Agency Name Secretary of State								
4. Records Series Item No.	5. Agency Item No.	6. Record Series Title	7. Retention Period			8. Archival	9. Remarks	10. 106 No.	11. TSLAC ONLY Amend. No.	
			Agency	Storage	Total					

3.4.007	2630	Return to Work Documentation	FE+5		FE+5				
3.4.008	2631	Sick Leave Pool Documentation	FE+5		FE+5				
5.4.011	2632	Visitor Control Registers	CE+3		CE+3				

Retention Codes (Field 7)	Archival Codes (Field 8)
AC – After Closed, Terminated, Completed, Expired, Settled AV – Administrative Value	A – Transfer to State Archives R – Review by State Archivist
CE – Calendar Year End FE – Fiscal Year End	PM – Permanent US – Until Superseded
LA – Life of Asset MO – Months	

The Office of the Secretary of State of Texas
Information Security Acknowledgement and Nondisclosure Agreement

User's Full Name

Section/Division/Organization

- As a user of the Office of the Secretary of State of Texas (SOS) information resources, I may have access to information that is private in nature or classified as Confidential or High Risk.
- I have read sections one and two of the SOS Information Security Policy and agree to follow the established guidelines.
- I will not disclose private, Confidential or High Risk information to unauthorized parties.
- Unless my job duties require, I will not access private, Confidential or High Risk information.
- I will not share my password used to logon to SOS computer systems or applications.
- I will not use a user identification code (System User ID) or password belonging to someone else.
- I will not enter any data or change any data that I do not have permission to enter or change.
- I will not use, load, install, or operate any software on an SOS owned computer or information resource without permission from the SOS Information Technology Division.
- I agree to immediately notify the SOS Information Technology Division if I know or suspect violations to the SOS Information Security Policy.
- I understand that any violations of the policy can result in disciplinary action, revocation of computer access, and may subject me to criminal penalties.

Signature of User

Date

I acknowledge that this employee, Contractor, Intern, Consultant, or any other temporary worker has been provided access to the SOS Information Security Policy. I also acknowledge that this employee has been provided only with the computer access needed to do his or her job.

Signature of User's Supervisor

Date

System User ID (assigned by administrator) _____

OFFICE OF THE SECRETARY OF STATE

Policies and Procedures Manual

2012

TABLE OF CONTENTS

PREFACE.....	i
SECTION 1 ORGANIZATION AND ADMINISTRATION	
Introduction	1
Organization and Duties of the Agency	1
Administration	4
SECTION 2 STANDARDS OF CONDUCT	
General	10
Ethics Advisor	10
General Conduct	10
Personal Interest, Outside Employment and Financial Activities	11
Acceptance of Gifts, Benefits and Favors	11
Political Activity	12
Political Contributions	13
Employment as a Lobbyist	13
Use of State Property	13
Use of Electronic Mail (E-Mail)	14
Use of Internet	17
Centralized Capitol Complex Telephone System	18
Reporting Losses Due to Fraudulent or Unlawful Conduct	19
Nepotism	19
Outside Employment	20
SECTION 3 EMPLOYMENT DISCRIMINATION AND ANTI-RETALIATION LAWS	
General	22
SECTION 4 ANTI-HARASSMENT AND HOSTILE FREE WORK ENVIRONMENT	
Harassment and Anti-Discrimination	25
Sexual Harassment and Anti-Discrimination Training	26
Complaint Procedure	26
Additional Enforcement Information	26
Disciplinary Action	27
Confidentiality	27
False Accusations	27
SECTION 5 EMPLOYEE RECRUITMENT AND SELECTION	
At-Will Employment	28

TABLE OF CONTENTS

Employment Recruitment and Selection	28
Recruitment and Selection Procedures	28
Process for Recruiting and Selecting an Applicant	29
Process for Approval of Job Posting	29
Evaluation of Employment Applications	30
Applicant Interviews	30
Employment Preferences	31
Qualifications for Veteran’s Preference	31
Qualification for Foster youth Preference	31
Applicants with a Criminal Record	31
Final Selection	32
New Employee Orientation	33
Initial Trial Period of Employment	33
SECTION 6 FAIR LABOR STANDARDS ACT STATE AND HOLIDAY COMPENSATORY TIME	
General	34
Determination of FLSA Status	34
Definitions	34
Employees Not Exempt From the FLSA	34
Employees Exempt from FLSA Overtime Provisions	35
State Compensatory Time	36
Holiday Compensatory Time	37
SECTION 7 SALARY ADMINISTRATION AND EMPLOYEE COMPENSATION	
General Information	38
New Hire Salary Rate	38
Promotions	38
Demotions	39
Salary Reduction for Disciplinary Reasons	39
Reallocations	39
Reclassifications	39
Merit Increase/One-Time Merit	40
Merit Salary Rate	40
Equity Adjustments	40

TABLE OF CONTENTS

Enhanced Compensation Award	41
Lateral Transfers	42
Temporary Assignment	42
Base Salary	42
Longevity Pay	43
Benefit Replacement Pay	44
SECTION 8 PAYROLL AND PERSONNEL REPORTING	
Payday	45
Payroll Adjustments for Employees on Leave Without Pay	45
Method of Receipt of Payment	45
Deductions from Gross Pay	46
SECTION 9 GENERAL LEAVE AND MISCELLANEOUS LEAVE PROVISIONS	
Authorization for Leave	47
Leave Summary	47
Annual Leave	47
Sick Leave	48
Sick Leave Pool	50
Extended Sick Leave	52
Leave without Pay	54
Military Leave	55
Parental Leave	55
Miscellaneous Leave	56
Transfer of Accrued Leave	58
Credit for Accumulated Annual Leave and Sick Leave	58
Absence from Work Because of Inclement Weather	58
SECTION 10 STATE EMPLOYEE HOLIDAYS	
General	60
Optional Holidays (Substitute Holiday Leave)	61
SECTION 11 FAMILY AND MEDICAL LEAVE	
Introduction	62
Employee Eligibility	62
Leave Entitlement	62
Definitions	63

TABLE OF CONTENTS

Maintenance of Health Benefits	64
Job Restoration	64
Notice	65
Certification	65
Military Family Leave Entitlements	66
SECTION 12 EMPLOYEE BENEFITS	
General	69
Insurance	69
Retirement and Death Benefit	70
SECTION 13 MILITARY EMPLOYMENT AND RE-EMPLOYMENT RIGHTS	
The Uniformed Services Employment and Re-employment Rights Act (USERRA)	72
State Re-employment Following Military Service	73
Military Leave Entitlements & Eligibility	74
SECTION 14 TRAINING, PROFESSIONAL DEVELOPMENT AND OTHER BENEFITS	
Acquired Immune Deficiency Syndrome (AIDS) and Human Immunodeficiency Virus (HIV) Awareness Education	76
Equal Employment Opportunity (EEO) Standards Training	76
Professional Development and Training	76
Obligations Assumed By Participating Employees	76
Parking	80
SECTION 15 GRIEVANCE POLICY	
Right to Present Grievance	82
Representation	82
Expenditures for Representatives of Grievants Prohibited	82
General Provision Procedures	82
Involuntary Termination Grievance	85
SECTION 16 OFFICE MANAGEMENT	
General Comments	86
Document Retention	86
Office Hours	86
Flex Time (Staggered Work Hours)	86
Telecommuting	87
Office Decorum	87

TABLE OF CONTENTS

Procurement	89
Seminars and Conferences	90
SECTION 17 PERSONNEL MANAGEMENT	
Employee Performance Evaluation	92
Disciplinary Action	93
Termination of Employment	96
Involuntary Termination	97
Exit Interview	98
Multiple Employment with the State	98
Arrest, Charging and/or Conviction of Agency Personnel	99
Employment Reference Checks/Verification of Employment	99
Changes in Personal Information	99
SECTION 18 BUILDING MANAGEMENT	
Emergency Procedures	101
Safety Systems	101
Security	101
Signs	102
Outside or Non-Profit Organizations	102
Solicitations Requested by Office of the Secretary of State	102
Modifications to Buildings or Offices	103
Building Maintenance	103
Accident Prevention Program	103
SECTION 19 TRAVEL	
Policies and Procedures	105
Travel Request	105
Advance Travel Payments	106
Multiple Advances or Reimbursements for a Travel Expense	107
Travel Voucher Documentation Requirements	107
Multiple Employee Travel	107
Attendance at Seminars and Conferences	107
Reimbursement of Travel Expenses	108
Reimbursement of Gasoline Cost	108
Transportation Allowance	108

TABLE OF CONTENTS

Meals and Lodging	111
State Business Calls on Personal Cell Phones	112
Travel Contract Restrictions	112
Travel Discounts	113
Incidental Expenses	114
Election Inspecting	114
Elections Inspectors Not Employees of the Agency But Are Working On Behalf Of the Agency	114
Travel Voucher	115
Ombudsperson Daily Travel	115
Direct Billing	116
SECTION 20 HIV/AIDS WORKPLACE GUIDELINES	
Purpose	117
Policy	117
Confidentiality	117
Education and Training	118
SECTION 21 AMERICANS WITH DISABILITIES ACT (ADA)	
Purpose	119
Definitions	119
Employment	119
Administration and Implementation	121
Dissemination of Policy	122
Confidentiality	122
ADA Grievance Procedure	122
Reasonable Accommodations	122
Employment Test	124
Written Job Descriptions	124
SECTION 22 RETURN TO WORK PROGRAM	
Policy Statement	125
Eligibility	125
Notification of Injury, Disability, or Serious Health Condition	126
Certification of Healthcare Provider	127
Status Reports During Leave	127

TABLE OF CONTENTS

Return to Work	128
Use of Paid Leave	130
Responsibilities of Agency Supervisors	131
Prohibited Actions	131
Definitions	133
SECTION 23 SUBSTANCE ABUSE (DRUG-FREE AND ALCOLHOL FREE WORKPLACE)	
Purpose and Goal	134
Covered Workers	134
Applicability	134
Definitions	134
Prohibited Behavior	135
Notification of Convictions	136
Searches	136
Consequences	136
Return to Work Agreements	137
Treatment	137
Confidentiality	138
Shared Responsibility	138
Communication	138
SECTION 24 SERVICE AWARDS	
Purpose	139
Objective	139
Policy	139
Notification	140
Presentation of Awards	140
Service Award Committee	140
Procedure to Purchase and Award	141
SECTION 25 SAFETY	
Introduction	142
Assignment of Duties, Responsibility, Authority and Staffing	142
Hazard Identification, Reporting and Evaluation	143
AED Description	144

TABLE OF CONTENTS

Employee Education	145
Safety Committee	148
Fire and Evacuation Procedures	148
Fire Wardens	149
Emergency Phone Numbers	150
Occupational Safety and Health	150
Safety Checklist	153
Safe Lifting Techniques	154
Employee Notice	155
Right of Employee	155
SECTION 26 NOTARIES WITHOUT BOND	
General	157
Qualification	157
Notary Supplies	158
Notary Stamp	158
Notary Record Book	158
Performing Notarizations	158
Transfer or Termination of Employment of Notaries without Bond	158
SECTION 27 SOCIAL MEDIA	
Overview	160
Approvals Required To Use Social Media for Agency Business	160
Authorized Communications	160
Acceptable Content	161
Unacceptable Content	161
Response to Questions/Comments	161
Posts and Comments Are Public Information	162
Information Request	162
Records Retention	162
Employee Use of Social Media	162
Personal Use	162
SECTION 28 UNEMPLOYMENT AND WORKERS' COMPENSATION	
Unemployment Compensation	164
Workers' Compensation	164

TABLE OF CONTENTS

Section 29 Indoor Air Quality

[Introduction](#).....165

APPENDICES

- Appendix A [Forms](#)
- Appendix B [Information Security Agreement](#)
- Appendix C [Training Matrix](#)

PREFACE

This Policy and Procedures Manual (“Manual”) of personnel policies is for use by employees of the Office of the Secretary of State (“Agency”). It supersedes any previous Manual.

Its purpose is to provide employees with general guidelines governing personnel-related matters, such as hiring, salary warrants, leave, grievances, equal employment, legislative controlled actions, and separations. It is not intended to give detailed answers or cover all possible situations or specifics of each job. Because of the need to accommodate changes in the Agency, the following policies and procedures are subject to change without notice. Any changes in the Agency's policies and procedures may modify, supersede, or eliminate the policies and procedures contained in this Manual

This Manual does not constitute an employment contract or a guarantee of employment. Nothing in this Manual constitutes the terms of an employment agreement, express or implied.

The Agency is an employment “*at will agency*,” and *employment is at the discretion of the Secretary of State*. This means that either the employee or the Agency can terminate the employment relationship at any time for any reason. Nothing contained in this Manual affects the “*employment-at-will*” status of Agency employees.

In addition to the policies contained in this manual, all employees are subject to the policies and procedures contained in the General Appropriations Act and the Texas Government Code.

Unless otherwise expressly stated, anywhere the terms “**include, includes, including**” or derivations thereof are used, they are not intended to be words of limitation but merely examples. Even where not expressly stated, such terms shall be interpreted not to be limited to the expressly stated items and instead to mean, for example, “**including (but not limited to)**.”

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 1: ORGANIZATION AND ADMINISTRATION

1.0 INTRODUCTION

The Office of the Secretary of State (“Agency”) is one of six constitutional offices that make up the Executive Branch of the Texas State government. The Agency complies with all state and federal laws, and its policies are intended to follow both the letter and spirit of the law.

The mission of the Agency is to provide a secure and accessible repository for public, business, and commercial records and to receive, compile, and provide information. Additionally, the Agency’s mission is to ensure the proper conduct of elections, to authorize the creation and registration of business entities, and to publish state government rules and notices. The Agency assists its staff with personal and professional development, and it promotes and develops a diverse workforce and makes effective use of resources.

The Agency shall provide accurate, reliable, and timely services. The Agency shall always act in accordance with the highest standards of ethics, accountability, efficiency, and openness. The Agency approaches its activities with a deep sense of purpose and responsibility.

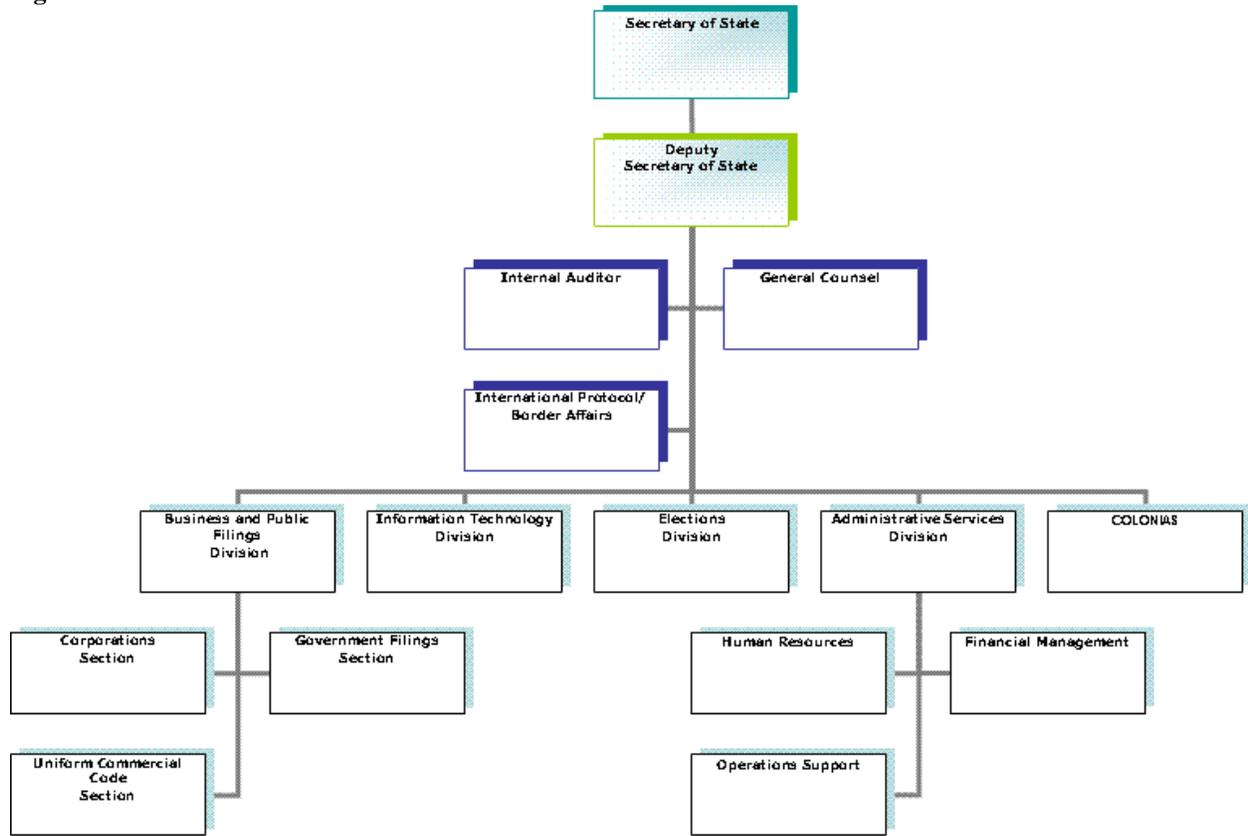
1.1 ORGANIZATION AND DUTIES OF THE AGENCY

The various duties and functions of the Agency are divided into the following five divisions: Executive, Elections, Information Technology, Business and Public Filings, and Administrative Services. The Executive Division is under the direction of the Secretary of State and the Deputy Secretary of State. The Elections, Information Technology, Business and Public Filings, and Administrative Services Divisions are each under the Executive Division but directly managed on a day-to-day basis under the direction of a director. Each director is under the direction of the Secretary of State and Deputy Secretary of State. See organization chart in Figure 1.

OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL

SECTION 1: ORGANIZATION AND ADMINISTRATION

Figure.1



**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 1: ORGANIZATION AND ADMINISTRATION

Executive Division

The Executive Division consists of the Secretary of State, the Deputy Secretary of State, and the General Counsel to the Secretary of State and their respective staffs.

Elections Division

The Secretary of State is the chief election officer for the State of Texas. The Elections Division provides assistance and advice to election officials on the proper conduct of elections. This includes hosting seminars and elections schools and providing calendars, ballot certification, primary election funding, and legal interpretations of election laws to election officials.

Information Technology Division

The Information Technology Division provides information technology and computer support for the Agency. It preserves electronic data related to business organizations, Uniform Commercial Code filings, the *Texas Register*, the Texas Administrative Code, notary public commissions, and voter registration activity. This is accomplished by maintaining a network of computers that support mission-critical applications, office automation, and access to external entities. This division also provides communication and computer support for special projects such as election night returns. Any personal or shareware software determined necessary by a director to perform Agency business must be reviewed by the Information Security Officer for virus protection and copyright compliance.

Business and Public Filings Division

The Business and Public Filings Division consists of three sections: Business Entity Filings, Government Filings, and Uniform Commercial Code.

- **Business Entity Filings** –Reviews and files documents that affect the existence, structure, or authority of domestic and foreign corporations, limited partnerships, limited liability companies, and registered limited liability partnerships, and assumed names for those organizations. This section also reviews trademarks and service marks.
- **Government Filings** –Acts as agent for service of process when required by statute, issues commissions for appointed and elected state officers for the Governor, and files and publishes the legislative bills passed by each legislative session. This section also commissions notaries public and files miscellaneous documents. The miscellaneous filings relate to health spas, automobile clubs, business opportunities, athlete agents, credit service organizations, and the private use of the state seal of Texas. This section publishes proposed and adopted rules in the *Texas Register* and an online publication, and compiles adopted rules in the Texas Administrative Code. In addition to agency rules, the *Texas Register* contains state agency open meeting agendas, notices of Governor’s appointments and executive orders, opinions of the Attorney

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 1: ORGANIZATION AND ADMINISTRATION

- General, election law opinions of the Secretary of State, and a wide array of other documents issued by state agencies.
- **Uniform Commercial Code** –Files documents submitted under Article 9 of the Uniform Commercial Code, the Uniform Federal Lien Registration Act, and Chapter 261 of the Texas Business and Commerce Code (concerning utility security instruments). Additionally, the section files restitution liens, aircraft maintenance liens, contract agricultural liens, transition property notices, and liens in favor of sellers of agricultural chemicals, agricultural seeds, and animal feed.

Administrative Services Division

The Administrative Services Division consists of the Financial Management Section and the departments of Human Resources, Purchasing, and Mailroom.

- **Human Resources Department (HRD)** –Handles all functions associated with job vacancy announcements, initiates all personnel actions, and provides assistance and counseling on all human resource-related matters.
- **Financial Management Section** –Handles the financial affairs of the Agency, which include the functions of accounting, budgeting, and payroll.
- **Purchasing Department** –Processes all of the Agency’s purchases and ensures that all purchases are in compliance with state and Agency policies.
- **Mailroom Department** –Provides Agency support for all incoming and outgoing mail on a daily basis.

1.2 ADMINISTRATION

The Secretary of State delegates authority to the Deputy Secretary of State for the day-to-day Agency operations.

Policy Formulation

Subject to the approval of the Secretary of State, the Deputy Secretary of State formulates or alters Agency policy.

The HRD will review the Policy and Procedures Manual (“Manual”) periodically and will update it as necessary. It outlines the employee’s responsibilities to the Agency as well as the Agency’s obligations to the employees. Both the Agency and the employee are ultimately responsible to the taxpayers of the State of Texas. The Secretary of State or the Deputy Secretary of State will approve recommendations for changes to comply with current laws, statutes, and regulations and to improve efficiency.

All prior rules, regulations, policies, and manuals of the Agency that may be in conflict are superseded by this manual, unless otherwise specified.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 1: ORGANIZATION AND ADMINISTRATION

Should any conflict arise between the policies established in this Manual and any statute of the state, such statute shall take precedence. If any section, subsection, paragraph, sentence, clause, or phrase of this Manual is found by a court of competent jurisdiction to be invalid or illegal, such findings shall not affect the validity of the remaining portions of this Manual.

These policies and procedures are subject to all applicable existing or future laws or regulations of the State of Texas and the Federal government (as amended from time to time). Wherever there is a conflict between the provisions of these policies and procedures and any applicable law or regulation, the provision of the law or regulation shall govern.

Supplemental policies and procedures that clarify or otherwise interpret the policies and procedures contained in this Manual may be established by divisions/sections for their employees subject to written approval of the Secretary of State or his/her designee. In the event of conflict between such supplemental policies and procedures and those contained in this Manual, the provisions of this Manual shall control. Either the Secretary of State or the Deputy Secretary of State may alter or waive any policies or procedures contained in this Manual at any time without prior notice. This Manual supersedes all previous Policies and Procedures Manuals and is available via the agency's intranet.

Management Transitions

To facilitate administrative transitions, the Executive Committee shall draft written status reports according to the wishes of the outgoing and incoming Secretaries of State. The transition/briefing reports detail the current status of Agency operations, projects in progress, and problems. A consistent format shall be utilized.

Agency Legislative Agendas/Relations

Only the Secretary of State has a legislative agenda with respect to Agency-related issues. Employees may appear as resource witnesses before legislative committees with respect to Agency-related issues only under a delegation of authority from the Secretary of State. Employees must promptly inform the Secretary of State as to the outcome of appearances before committees.

Absent an express delegation of authority, employees of the Agency may not initiate contact with the Legislature regarding Agency legislative issues without the prior knowledge and consent of the Secretary of State. Contacts with employees initiated by the Legislature or relating to legislation of interest to the Agency must immediately be reported to the Secretary of State.

The Administrative Services Division coordinates all information transmitted to the Legislature pertaining to appropriations and to budget requests, including fiscal notes on legislative bills.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 1: ORGANIZATION AND ADMINISTRATION

Legal Matters

The Deputy Secretary of State and the General Counsel to the Secretary of State coordinate legal affairs for the Secretary of State and should be advised of any sensitive issues, potential litigation, policy development, or any subpoena requiring the personal appearance of an employee of the agency.

Internal Audit

The Internal Auditor shall be responsible for performance audits of the SOS. Performance audit is defined as an independent appraisal activity performed by the Internal Auditor that includes determining whether the entity being reviewed is acquiring, protecting, and using its resources economically and efficiently, identifying the causes of inefficiency or uneconomical practice, and determining whether the entity has complied with laws, rules, and regulations.

The Secretary of State shall select the Internal Auditor.

- The Internal Auditor shall report directly to the Secretary of State or his/her designee.
- The Secretary of State or his/her designee shall be responsible for the administrative supervision of the internal audit program.
- The Secretary of State or his/her designee shall ensure the independence of the internal audit function.

The Internal Auditor shall submit to the Secretary of State for approval the annual audit plan, which shall be based on risk analysis and which shall identify individual audits to be performed during the year. Special audit projects not included in the approved annual audit plan may be authorized by the Secretary of State.

On a basis determined by the Secretary of State, the Internal Auditor shall meet with the Secretary of State or his/her designee to discuss the status of implementing the Internal Audit Plan, including exceptions to the timely accomplishment of the plan, the status of management's resolution of audit findings, and other significant issues involving the internal audit function.

The Internal Auditor's activities in reviewing, appraising, and reporting established policies, plans, and procedures shall not in any way relieve SOS personnel of responsibilities assigned to them.

The implementation of, or action taken on, the Internal Auditor's recommendations shall be the duty of SOS management. The Internal Auditor will perform follow-up audits to determine what corrective action was taken and whether it is achieving the desired results.

The agency's internal audit program will undergo a peer review at least every three years to comply with the requirements established in the Texas Internal Auditing Act.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 1: ORGANIZATION AND ADMINISTRATION

Intellectual Property

Manuals, guides, software, and other material in which the Agency may have a proprietary interest shall be protected by copyright. The Deputy Secretary of State or his/her designee shall coordinate the copyright protection process.

It is the policy of the Agency to honor all vendor copyrights. Accordingly, all requests for copies of system or application software or requests for any information regarding any computer-related product utilized by this Agency must be approved by the Information Technology Division.

The Information Technology Division investigates all such requests and reports to the originator whether the request is approved or denied due to copyright protection laws. The advice of the Deputy Secretary of State shall be obtained as necessary.

Materials developed by an employee in the course and scope of the employee's employment or, if not in the course and scope of such employment, that utilized any state resources shall, however minimal, be the property of the Agency. "Materials" includes any intellectual property, such as copyrights or trademarks, retained in or otherwise related to the materials. The policy also covers such items as a list of contacts or compiled phone lists that were created in the course of state employment.

Media Relations

Routine requests for information shall be handled by the persons designated to respond to public inquiries for the requested information irrespective of whether the requesting party is a member of the press. For example, routine requests for information include election dates and results, database information and information from documents on business organizations, financing statements, notary commissions, administrative rules and regulations, dates of employment, and other information routinely provided to members of the public.

Requests from members of the press that do not involve merely the routine provision of information as outlined above or which involve a sensitive issue shall be referred to the Director of Communications. Requests from members of the press of a legal nature shall be referred to the General Counsel or Director of Communications. Any controversial matter or any question involving an opinion, interpretation, or statement of policy to be attributed to the Secretary of State shall be forwarded to the Director of Communications.

This policy is not intended to limit the access of the press to public information, but rather to ensure that opinions, interpretations, and policy statements attributed by the media to the Secretary of State are in fact those of the Secretary of State. Additionally, the policy serves to alert Executive Management to sensitive or controversial matters which might require its attention.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 1: ORGANIZATION AND ADMINISTRATION

As with all provisions of public information, employees must ensure that the information provided is accurate, reliable, and timely.

Purchase of Technology/Computers

The Information Technology Division shall review all requests relating to the utilization of electronic information processing, hardware, software, services, and personnel (excluding temporary personnel) prior to the execution of any contracts or agreements between the Agency and any other entity.

Purchasing

The Purchasing Department shall make all commitments to purchase supplies, material, equipment, and services. Contracts shall be made only when based upon a properly approved purchase requisition. All purchase requisitions must be approved by a director. The Deputy Secretary of State must approve all requisitions in excess of \$1,000. Additionally, purchase requests for computers/technology must be reviewed by the Information Technology Division.

The Purchasing Department shall evaluate all requisitions for:

- Economic order quantities
- Compatibility with existing supplies or equipment
- Compliance with Agency standardization objectives
- Reasonable quality,
- Reasonable delivery dates, and
- Maximum utilization of state contracts.

All credit card purchases must be approved by the Purchasing Department after receipt of a properly approved purchase requisition. Credit cards will be issued to designated employees and then returned to the Purchasing Department after procurement of goods.

Expenditures

The primary control over expenditures is in the requisition and travel authorization processes. The Financial Management Section shall exercise secondary control over expenditures through review of invoices. Approval of all types of payment vouchers is delegated to the Administrative Services Division. The Secretary of State and/or the Deputy Secretary of State shall be maintained as authorized signatories for expenditures through the Comptroller of Public Accounts.

Staffing

Prior to submission to the Deputy Secretary of State, all changes to staffing shall be reviewed by the Human Resources Manager and the availability of requisite funds shall be confirmed by the Director of Administrative Services.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 1: ORGANIZATION AND ADMINISTRATION

Correspondence

All written communications should be as concise and simple as possible. Please avoid the use of jargon. Form letters and other written correspondence or documents may be signed on behalf of the Secretary of State or Deputy Secretary of State through the use of an electronic or autopen signature. The Secretary, Deputy, or a designee must approve in advance the form of the documents to be signed in this manner.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 2: STANDARDS OF CONDUCT

2.0 GENERAL

This policy does not supersede any state law regulating the ethical conduct of state employees. While this policy provides general guidelines for agency employees in regard to ethical questions, it is not legal advice. Employees should consult the Ethics Advisor for guidance when specific ethical issues arise.

An employee violating any provision of this policy may be subject to discipline, including termination.

2.1 ETHICS ADVISOR

The Secretary of State designates the General Counsel as the Agency's Ethics Advisor. The Ethics Advisor shall serve as a liaison between the Agency and the Texas Ethics Commission. The Ethics Advisor shall also be available to consult individually with Agency employees on particular ethics questions that may arise. Employees may also e-mail questions or comments to the General Counsel at EthicsQuestion@sos.state.tx.us.

2.2 GENERAL CONDUCT

- Employees shall always treat members of the public with dignity and respect.
- Employees shall avoid any action that may result in or give the appearance of using the position of public servant for private gain.
- Employees shall avoid any action that may adversely affect the public's confidence in government.
- Employees shall not use or possess illegal or dangerous drugs.
- Employees shall abstain from the use of alcoholic beverages while on duty or while off duty when return to duty is imminent (e.g., during a meal break when return to work is planned).
- Employees shall not report to work or operate any state vehicle when evidence of the use of alcohol may be detected.
- Employees shall utilize state equipment for state purposes and shall follow state regulations and procedures regarding maintenance and use of state property.
- Employees may make incidental personal use of work telephones for local calls, as there is no additional cost or damage to the state from such use.
- Employees shall charge their personal calling cards or home numbers for costs incurred when making personal or non-state-related long distance calls on state work phones.
- Employees shall reimburse the state for long distance calls made under emergency circumstances on work telephones.
- Employees' excessive use of work telephones for personal or private matters may be the basis for disciplinary action.
- Employees shall not participate in gambling, betting, or lotteries on state property.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 2: STANDARDS OF CONDUCT

- Employees shall not provide false statements or false information in any area of official duty to fellow employees or to the general public.
- Employees shall submit truthful and complete reports. Employees reporting false information shall be subject to severe disciplinary action that may include termination.
- Employees shall not remove, conceal or falsify governmental records. Destruction of governmental records shall be permitted only under records retention guidelines.
- Employees shall not use state-issued credit cards for expenses that are clearly personal in nature and not necessitated by or incidental to state business.
- Employees may charge expenses on state-issued credit cards for expenses necessitated by or incidental to state business (e.g., hotel costs in excess of per diem, toiletries, tips, and movie charges) but may not seek reimbursement from the state for those expenses.
- Employees may use “frequent flyer” mileage accrued on state business for personal travel.

2.3 PERSONAL INTERESTS, OUTSIDE EMPLOYMENT, AND FINANCIAL ACTIVITIES

- Employees must obtain written approval from their supervisors and section/division directors prior to accepting outside employment or self employment.
- Employees shall not have any interest or engage in any financial activity or employment that conflicts with the performance of their duties for the state.
- Employees must obtain written approval from their supervisors and section/division directors prior to participating in outside financial activities that may appear to conflict with their position as public servant.
- Employees shall not accept any employment or compensation that could influence their judgment or hinder their independence of judgment in the performance of their official duties.
- Supervisors shall not be involved in outside employment or financial interests with employees under their supervision.
- Employees shall not accept other employment or engage in financial or professional activities that could require or cause them to reveal confidential information acquired through their official positions.
- Employees shall not make personal investments that create a conflict between their personal interests and the public interest.

2.4 ACCEPTANCE OF GIFTS, BENEFITS AND FAVORS

CAUTION: *If any gift is offered in exchange for action or inaction on the part of the employee, that gift would be considered the basis for a bribe.*

- Employees shall not solicit or accept any benefit, gift, favor, or service that might influence them in the performance of their duties.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 2: STANDARDS OF CONDUCT

- Employees shall not solicit or accept any benefit, gift, favor, or service that they know is being offered with the purpose of attempting to influence their official conduct.
- Employees shall not solicit or accept any benefit, gift, favor, or service for having performed their official duties in favor of another.
- Employees shall not solicit or accept any benefit, gift, favor, or service from a person who is seeking to obtain business from or financial relations with the Agency.
- Employees shall not solicit or accept any benefit, gift, favor, or service from a person seeking employment with the Agency.

Each of the following exceptions is subject to the preceding prohibitions. The prohibited conduct always supersedes any exception.

- Employees may accept gifts or benefits from family members.
- Employees may accept gifts or benefits from their personal friends so long as the gift is not intended to influence the employees' official conduct.
- Employees may accept gifts or benefits from professional or business relationships independent of the official status of the recipient as public servant (e.g., an insurance agent, accountant, etc.) so long as it is not intended to influence official action as public servant.
- Employees may accept items that are under \$50 in value (e.g., lunch, key chains, mugs, tee shirts, and caps). Employees may not accept cash, checks, money orders, other negotiable instruments, or cash equivalents, including but not limited to gift certificates and prepaid bank or phone cards.
- Employees may accept small amounts of perishable foods or plants delivered infrequently by donors.
- Employees shall not accept any gifts or benefits from a lobbyist that are over \$50 in value.
- Employees may accept food or refreshments from lobbyists in the context of a legislative reception.
- Employees may accept benefits from lobbyists on an infrequent basis as long as the benefits are unsolicited and under \$50 in value.
- Employees who frequently accept benefits from lobbyists contrary to these guidelines may be subject to disciplinary action.

2.5 POLITICAL ACTIVITY

- Employees shall not engage in any political activity during regular working hours unless on approved annual leave or its equivalent (e.g., compensatory or holiday time).
- Employees shall not wear political name badges or other paraphernalia while on duty.
- Employees shall not display political paraphernalia in their offices.
- Employees, in exercising their personal political rights, must avoid any implication that their political activities represent the official position of the Agency.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 2: STANDARDS OF CONDUCT

- Employees shall not use any state funds to influence the outcome of any election or legislation. Testimony before legislative committees or registration in support of or in opposition to legislation not relevant to the Agency must be done on an employee's own time (e.g., annual leave, compensatory time, etc.).

2.6 POLITICAL CONTRIBUTIONS

Employees are free to make political contributions to the candidates of their choice and should be aware that federal and state laws govern the amount and timing of these contributions. Employees may not solicit political contributions from other employees.

2.7 EMPLOYMENT AS A LOBBYIST

No employee can be employed as a lobbyist (paid or unpaid) while employed by the Agency.

2.8 USE OF STATE PROPERTY

State property is to be used only for conducting state business only and may not be used for personal reasons. The appropriation of state property for personal use may be grounds for disciplinary action up to and including termination.

Information Resources

The Information Security Policy (Appendix B) governs the use and protection of Agency information resources. All users of Agency resources are required to read sections one and two of the Information Security Policy and submit to the HRD the **Information Security Acknowledgement and Nondisclosure Agreement**, which is located in Appendix A.

Employees may contact the Information Security Officer for questions, issues, or to report a potential security incident. Employees may also send an e-mail to [Information Security](#).

- **Personal Calls** – The telephones in the Agency offices are for business use. Personal calls using an Agency phone or personal cell phone must be kept to a minimum and are permissible for emergency situations or in situations that cannot wait until the end of the day (e.g., calls to day-care service, doctor, or to a spouse or child). This personal use should be infrequent and limited to breaks and lunchtime, except in the case of an emergency. During office hours, personal communication devices such as cell phones and beepers must not be disruptive to the business environment. No personal long distance calls are to be made on the CCCTS or directly charged to a telephone number of the Agency. Such calls are a misappropriation of state funds and may be grounds for disciplinary action including and up to immediate termination.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 2: STANDARDS OF CONDUCT

- Consumable Supplies - Consumable supplies are purchased by each section/ division for state use and should not be used by the employee for personal purposes.
- State Letterhead - The use of state stationery by any Agency employee is permitted only for purposes related to Agency business. The use of state stationery by any Agency employee for purposes unrelated to Agency business is prohibited.
- Section/division directors may use state stationery to write a letter of recommendation for current or former employees of the Agency with whom such manager(s) has/had direct professional contact during the employee's tenure. Only managers may write letters of recommendation on state stationery, and they may do so only under the circumstances described in the immediately preceding sentence. Under such circumstances, letters of recommendation are considered to be related to Agency business.
- Postage and Mail - All general postage for the Agency shall be metered. No personal mail shall be run through the postage meter nor shall any outgoing personal mail be processed by the Agency mailroom.
- Printing and Photocopying - The use of any reproduction equipment of the Agency is limited to official state business. No personal printing or photocopying is permitted.
- Facsimile machines - The use of the Agency facsimile machines is limited to official state business. Personal faxes may not be transmitted from Agency machines.
- Furniture, Equipment, and Books - Most furniture and equipment owned by the Agency must be inventoried at least annually. Custodial responsibility for Agency property is assigned to section/division directors. Furniture, equipment, and books may not be moved or transferred to another section/division without the approval of the section/division from which such items are to be moved. Section/division directors must appoint an inventory clerk to assist in maintaining accountability for property. Furniture, equipment, and books should not be used for personal purposes.
- Receipt of Personal Mail and Packages - Employees are not to give the address of the Agency to others for the purpose of receiving personal mail and packages at the workplace.

2.9 USE OF ELECTRONIC MAIL (E-MAIL)

The Agency provides its employees and certain vendors (employee-users) with electronic mail communications. The primary purpose of the electronic mail system is to expedite necessary business communications between two or more individuals. As such, the use of electronic mail is for the Agency's business purposes. Use of e-mail is a privilege and may be revoked at any time. Use of e-mail constitutes acceptance of this policy.

Employees and employee-users are expected to be knowledgeable of these policies of the Agency. Any questions should be directed to the Information Security Officer (ISO). Violations of this or any other policy subjects the employee and employee-user to immediate revocation of system privileges and may result in disciplinary action, up to and including termination. Any information included in e-mail communications becomes

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 2: STANDARDS OF CONDUCT

the property of the Agency and is subject to monitoring for compliance with all Agency policies by the ISO and the Internal Auditor.

The Agency reserves and intends to exercise the right to review, audit, intercept, access, and disclose all messages created, received, or sent over the electronic mail system for any purpose. The contents of electronic mail properly obtained for legitimate business purposes may be disclosed within the Agency without the permission of the employee.

The confidentiality of any message should not be assumed. Even when a message is erased, it is still possible to retrieve and read that message. Further, the use of passwords for security does not guarantee confidentiality. User account passwords must not be divulged to anyone.

Notwithstanding the Agency's right to retrieve and read any electronic mail messages, such messages should be treated as confidential by other employees and accessed only by the intended recipient. Employees are not authorized to retrieve or read any e-mail messages that are not sent to them. Any exception to this policy must be approved by the Deputy Secretary of State.

E-mail Accounts

Employees and employee-users must first be authenticated through an Agency-assigned network username and password. The username and password is the responsibility of the individual to whom it is assigned. Any authorized use of the username and password by other individuals (i.e., family members) to gain access to the Agency network and Internet makes that user responsible for any and all actions of the individuals.

An electronic mail "account" is assigned to each employee-user. Any communication sent from that account is the responsibility of the employee-user assigned to the account. Employee-users are prohibited from allowing other individuals to send electronic mail from their account and may not use another account to send e-mail communications for their own purposes. You should not expect that electronic mail communications made through the Agency system are confidential. Although you will be given a username and password this does not insulate transmission from employer review.

Personal Use

As stated previously, the use of electronic mail through the Agency network is primarily for business purposes. Incidental personal use of the electronic mail system is permitted. However, the personal use of e-mail should not interfere with Agency operations, nor should it cause any harm or embarrassment to Agency. Any personal use of e-mail is expected to be on the employees' own time and is not to interfere with their job responsibilities.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 2: STANDARDS OF CONDUCT

Proper and Ethical Use of Electronic Mail

At any time and without prior notice, Agency management reserves the right to examine e-mail, personal file directories, and other information stored on Agency computers. This examination helps to ensure compliance with internal policies, supports the performance of internal investigations, and assists with the management of Agency information systems. As such, the ISO or any representative of the ISO may monitor the content of electronic mail. Use of the electronic mail system constitutes acceptance of such monitoring.

This policy should be read and interpreted in conjunction with all other Agency policies including but not limited to policies prohibiting harassment, discrimination, offensive conduct, or inappropriate behavior. Employees are prohibited from using electronic mail for any unethical purposes, including but not limited to pornography, violence, gambling, racism, harassment, or any illegal activity. Employees are forbidden from using profanity or vulgarity when posting electronic mail.

Employees are also prohibited from using electronic mail through Agency systems for any other business or profit-making activities. Disclosure of any confidential information through electronic mail to any party not entitled to that information is prohibited.

Employees are prohibited from entering into any contracts or agreements on behalf of the Agency through electronic mail. Any such contracts or agreements must be executed through normal channels and must be expressly authorized by management.

Employees shall not use a code, access a file, or retrieve any stored information, unless authorized to do so. Employees should not attempt to gain access to another employee's messages without the latter's permission.

In general, employees should exercise the same restraint and caution in drafting and transmitting messages over the electronic mail as they would when writing a memorandum and should assume that their messages will be saved and reviewed by individuals other than the intended recipients.

Transmitting E-mail to "Everyone" Group

Employees are prohibited from sending electronic mail to all other employees through the use of the "SOS Employees" address group unless expressly authorized by management to do so. Excessive use of this address group strains the network.

Electronic Mail Through the Internet

Employees may be authorized to transmit or receive electronic mail to and from individuals through the Internet (outside of Agency's network). Employees should take extreme caution when using the e-mail in this manner. All files or software should be passed through virus protection programs prior to use. Failure to detect viruses could

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 2: STANDARDS OF CONDUCT

result in corruption or damage to files and/or unauthorized entry into the Agency's network. It is mandatory that employees comply with copyright and trademark laws when downloading materials from the Internet. To obtain detailed information regarding the obligations and responsibilities of employees while communicating through the Internet, please refer to the Agency's Internet Use Policy.

If an employee discovers that any damage occurred as a result of downloading software or files, the incident should be reported immediately to the ISO.

2.10 USE OF THE INTERNET

Internet access is provided to employees as an informational tool to enhance the efficiency and performance of the employee's duties. Like e-mail, the Internet is to be used for conducting Agency business and may be accessed for limited personal use only on an infrequent basis during breaks subject to appropriate use and conflict-of-interest policies. In no event may an employee use Agency Internet for inappropriate purposes. Inappropriate use or abuse of Agency Internet resources shall subject the employee to disciplinary action including immediate termination of employment.

The Agency reserves the right to review the Internet sites accessed or visited from Agency computers, including for the purpose of investigations of possible misconduct or abuse and to ensure that the Agency's resources are devoted to maintaining the highest levels of productivity.

Definition of "Inappropriate"

Agency policy does not permit any inappropriate use of Agency e-mail or Internet resources, regardless of how limited or infrequent the use, or regardless of whether the use occurs during business hours or outside normal business hours. Inappropriate use includes sending, receiving, accessing, reading, viewing, or listening to materials (auditory, verbal, or visual), messages, images, or pictures of a sexual nature; or communications that promote hatred, harassment, illegal activity, or discrimination on the basis of sex, race, religion, national origin, age, or disability.

The Secretary of State has a policy of zero-tolerance regarding inappropriate use of Agency e-mail or Internet resources. Employees engaging in inappropriate use of e-mail or Internet resources will be subject to disciplinary action up to and including immediate termination of employment.

Public Information

Electronic records on Agency computers are subject to the Texas Public Information Act. Employees should not consider any information on assigned computers to be private or confidential or personal property of the employee. See Acceptable Use Policy and Privacy Policy in Section 2 of the Information Security Policy (Appendix B).

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 2: STANDARDS OF CONDUCT

Cost to the Agency

While some limited personal use of the Agency's e-mail and Internet resources is permissible, no personal use of these resources may cause the Agency to incur any costs. Hence, printing of personal e-mail or information from personal Internet use is prohibited.

Agency Owned Communication Devices

Employees who are assigned communication equipment (e.g., PDA) for use in the performance of their duties are to use these devices only for job-related business and activities. All Agency communication devices will be inventoried on a yearly basis and will need to be accessible during the agency physical inventory. All PDAs and other communication equipment must be relinquished to HRD upon separation from the Agency. Lost or damaged property must be reported to the Purchasing Department immediately. In certain instances, employees may be liable for the replacement of the lost or damaged property. Use of these devices for personal reasons is misappropriation of state funds and may be grounds for disciplinary action including immediate termination of employment.

Cell Phones

The Agency provides cellular telephone service on communication devices issued by the Agency. The use of this service is limited to designated personnel.

Employees may be reimbursed for state business calls made on the employee's personal cell phone. The basis of a reimbursement request will be a copy of the employee's itemized cell phone bill upon which the employee has designated state business calls. To be reimbursable, the state business call must have caused an incremental cost over and above the cost of the employee's basic plan. The Agency will not reimburse for state business calls which are within the employee's base plan.

2.11 CENTRALIZED CAPITOL COMPLEX TELEPHONE SYSTEM ("CCCTS")

Local calls – The Capitol exchange, CCCTS, includes the numbers of most state agencies in the Capitol area. An employee can dial CCCTS stations directly without using the 463, 475, 936 or 305 prefixes. Dial 3 + the 4-digit station number if the number has a 463 prefix. Dial 5 + the 4-digit station number if the number has a 475 or 305 prefix. Dial 6 + the 4-digit station number if the number has a 936 prefix.

Long Distance Calls – To make a long distance business call, dial 9 + the area code and number. (Example: 9-817-799-3611) Dial the area code even if it is the same as the number from which the call is placed. By dialing in this manner, one accesses the State of Texas Network, resulting in the most economical use of state phone lines.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 2: STANDARDS OF CONDUCT

2.12 REPORTING LOSSES DUE TO FRAUDULENT OR UNLAWFUL CONDUCT.

Under Chapter 321 of the Government Code, the Secretary of State is required to report to the State Auditor when money received by the Secretary of State or a client or contractor of the state may have been lost, misappropriated, or misused. Further, the Secretary of State is required to file a report when it is determined that there is reasonable belief that other fraudulent or unlawful conduct has occurred in relation to the operation of the Agency.

When employees have reasonable cause to believe that fraudulent or unlawful conduct has occurred or that money received by the office has been lost, misappropriated, or misused:

- Employees must promptly report this loss to the section/division director.
- If the suspected conduct is on the part of the section/division director, employees must report the suspected conduct to the next level of management or to the Director of Administrative Services.
- The Director of Administrative Services shall promptly notify Executive Management of the report of fraudulent or unlawful conduct. After reviewing the report, Executive Management shall determine the appropriate actions necessary to resolve the allegations. Executive Management may refer the matter for investigation to the Internal Auditor, General Counsel, or another person designated by the Executive Management.

It is incumbent upon employees to ensure that reports under this provision are prompt and are not malicious or knowingly false. It is incumbent upon management to promptly refer matters to Executive Management to ensure that the identities of the employees reporting under this provision will be kept confidential to the extent possible and as required by law and that there is no retaliation against any employee making a good faith report.

If employees experience a loss of personal property due to suspected theft, employees should report the loss to the section/division director and to the Human Resources Manager. The Human Resources Manager will notify the Department of Public Safety of the suspected theft. To ensure the safety of the employees and the personal property of the employees, the HRD will track all reports of thefts or other security issues.

2.13 NEPOTISM

No one may be appointed, assigned, or hired under the direct or indirect supervision and/or personnel management accountability of a relative or where the relative controls the employee's compensation, work assignments, working conditions, or hours of work. No person who is a relative of another may be in a position that has access to confidential information that might affect either employee's employment position. Also, a

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 2: STANDARDS OF CONDUCT

manager/team leader may not supervise two employees who are relatives. A relative means someone related by consanguinity (of any degree) or by affinity if they are married to each other or if the spouse of one of the individuals is related by consanguinity to the other person. Adopted children, step children, and step parents are relatives for the purposes of the Agency's nepotism policy.

The Agency will not employ relatives of any kind, whether by consanguinity or affinity, to any degree to work in the same section or division of the Agency. Furthermore, the Agency discourages the employment of relatives in any case where the employment might reasonably present a conflict with employees or potential employee's duties and responsibilities to the Agency due to the relationship. Any interpersonal relationships not specifically addressed by the Agency's nepotism policy will be reviewed and addressed, as necessary, to avoid the possibility of conflicts between those personal relationships and the employees' duties and responsibilities to the Agency.

The Agency will not authorize or approve the transfer or promotion of an employee in any division, or between divisions, that would result in a family member having authority over another family member in the manner prohibited above by this policy, either directly or indirectly. The Agency will transfer, if practical, or terminate employees when the marriage of the employees or other changes in family relationships results in a violation of the Agency's nepotism policy. In making its decisions regarding the effect of such a marriage or other changes in family relationships, the Deputy Secretary of State will consider the circumstances involved and the best interests of the Agency.

Each employee is required to immediately inform his/her team leader and manager and the HRD of any change in marital or other family relationship that might create a violation of this policy. Team leaders and managers will keep the HRD informed regarding any potential violations of the Agency's nepotism policy of which they become aware. All individuals who apply for employment with the Agency must disclose whether they have any relatives, whether by consanguinity or by affinity, that work for the Agency. Each current employee is also responsible for immediately disclosing to the HRD notice of a relative who is an applicant for a job with the Agency. Failure to make the disclosures required in this paragraph may result in disciplinary action including and up to termination or rescinding an offer of employment by the Agency.

The Deputy Secretary of State or his or her designee must approve any exceptions to this policy.

2.14 OUTSIDE EMPLOYMENT

Employees are permitted to engage in outside work or hold other jobs, subject to certain restrictions as outlined below.

- Activities and conduct away from the job must not compete, conflict with, or compromise the Agency's interests or adversely affect job performance and the

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 2: STANDARDS OF CONDUCT

ability to fulfill all responsibilities to the Agency. Employees are prohibited from performing any services for customers on nonworking time that are normally performed by the Agency. This prohibition also extends to the unauthorized use of any Agency equipment and the unauthorized use or application of any confidential information. In addition, employees are not to solicit or conduct any outside business during paid working time.

- Employees are cautioned to consider carefully the demands that additional work activity will create before accepting outside employment. Outside employment will not be considered an excuse for poor job performance, absenteeism, tardiness, leaving early, refusal to travel, or refusal to work overtime or different hours. If outside work activity causes or contributes to job-related problems, it must be discontinued, and, if necessary, normal disciplinary procedures will be followed to deal with the specific problem.
- In evaluating outside work, the Secretary of State or Deputy Secretary of State and the HR department will consider whether the proposed employment:
 - May reduce the employee's efficiency in working for the Agency;
 - Involves working for an organization that does a significant amount of business with the Agency, such as major contractors, suppliers, and customers;
 - May adversely affect the Agency's image;
- Employees who have accepted outside employment may not use paid sick leave to work on the outside job. Fraudulent use of sick leave will result in disciplinary action up to and including termination.
- Employees must submit to the Secretary of State/Deputy Secretary of State through the employee's section/division director an Outside Employment Approval form (See Appendix A).

SECTION 3: EMPLOYMENT DISCRIMINATION AND ANTI-RETALIATION LAWS

3.0 General

Employment discrimination laws make it illegal for employers to treat employees and applicants adversely based on race, color, sex, religion, national origin, physical disability, age, or genetic information. The main body of employment discrimination laws is composed of federal and state statutes. This section summarizes some important federal and state laws that are applicable to state agencies.

Texas Workforce Commission, Civil Rights Division

The Texas Workforce Commission's Civil Rights Division (CRD) is responsible for the education on and enforcement of certain state and federal employment laws. They serve as the state Fair Employment Practices agency that is authorized, with respect to unlawful employment practices, to seek relief, grant relief, and institute criminal proceedings related to state and federal employment laws.

All new employees are required to receive training on policies and procedures regarding employment discrimination and sexual harassment no later than 30 days after the date of hire. In addition, all employees are required to receive supplemental training every two years thereafter. Employees are required to sign a statement verifying receipt of training, which will be maintained in each employee's personnel file.

An employee or applicant claiming to be discriminated against or aggrieved by an unlawful employment practice, or the person's agent, may file a complaint with the CRD.

Employees should be aware of the following principal employment laws not otherwise discussed in detail in this manual.

Americans with Disabilities Act of 1990 (ADA)

The Americans with Disabilities Act of 1990 (ADA) gives civil rights protections to individuals with disabilities similar to those provided to individuals on the basis of race, color, sex, national origin, age, and religion. It guarantees equal opportunity for individuals with disabilities in public accommodations, employment, transportation, state and local government services, and telecommunications.

This law prohibits discrimination in all employment practices, including job application procedures, hiring, firing, advancement, compensation, training, and other terms, conditions, and privileges of employment.

Americans with Disabilities Act Amendments Act of 2008 (ADAAA)

The Americans with Disabilities Act Amendments Act of 2008 (ADAAA) clarifies and broadens the definition of disability and expands the population eligible for protections under the Americans with Disabilities Act of 1990.

SECTION 3: EMPLOYMENT DISCRIMINATION AND ANTI-RETALIATION LAWS

Age Discrimination in Employment Act of 1967 (ADEA)

The Age Discrimination in Employment Act of 1967 (ADEA) and the Texas Labor Code prohibit discrimination against a person (employee or job applicant) because of his or her age with respect to any term, condition, or privilege of employment including, but not limited to, hiring, firing, promotion, layoff, compensation, benefits, job assignments, and training. Employees aged 40 and older are protected from such age-related discrimination. In addition, employees are not required to retire at any specific age.

Equal Pay Act of 1963 (EPA)

The Equal Pay Act (EPA) requires that men and women be given equal pay for equal work in the same establishment. The jobs need not be identical, but they must be substantially equal. It is job content, not job titles, that determines whether jobs are substantially equal. Employers may not pay unequal wages to men and women who perform jobs that require substantially equal skill, effort, and responsibility and that are performed under similar working conditions within the same establishment.

Federal Pregnancy Discrimination Act of 1978

The Federal Pregnancy Discrimination Act of 1978 and the Texas Labor Code prohibit discrimination on the basis of pregnancy, childbirth, or related medical conditions. Women affected by pregnancy or related conditions must be treated in the same manner as other employees or applicants who have medical conditions that place a similar limitation on their ability to or availability for work.

Genetic Information Nondiscrimination Act of 2008

The Genetic Information Nondiscrimination Act (GINA) of 2008 is a federal law that prohibits discrimination in health coverage and employment based on genetic information. GINA prohibits group health plans and health insurers from denying health insurance coverage or charging higher premiums based solely on a genetic predisposition. GINA also prohibits employers from using an individual's genetic information when making hiring, firing, job placement, or promotion decisions.

Texas Whistle Blower Act

The Agency may not suspend, terminate, or take other adverse personnel action against an employee who, in good faith, reports a violation of the law by the Agency or another public employee to an appropriate law enforcement authority. Employees can learn of their rights by viewing the Texas Whistle Blower Act poster in the Human Resources Department.

Texas Workers' Compensation Act

The Texas Workers' Compensation Act enables an employee who has been injured at work or has a work-related illness to receive medical benefits as well as income benefits. In addition, it protects against discrimination based upon workers' compensation claims history

SECTION 3: EMPLOYMENT DISCRIMINATION AND ANTI-RETALIATION LAWS

Religious Affiliation Discrimination

Texas Labor Code, Chapter 21, prohibits discrimination against an employee or applicant based on any aspect of religious observance, practice, or belief unless the Agency demonstrates that the Agency is unable reasonably to accommodate the religious observance or practice of an employee or applicant without undue hardship to the conduct of the Agency's business.

More detailed information on the above laws and other mandatory employment posters are located in the Human Resources Department.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 4: ANTI-HARASSMENT AND HOSTILE-FREE WORK ENVIRONMENT

4.0 HARASSMENT AND ANTI-DISCRIMINATION

The Agency is committed to providing equal employment opportunities and a workplace free of any form of harassment and discrimination. Employment discrimination on the basis of race, color, national origin, sex, religion, age, mental or physical disability, military status, retaliation, and any other characteristic protected by applicable federal or state law is strictly prohibited.

The Agency does not tolerate harassment of any nature that results in a hostile work environment. Employees are expected to maintain a productive work environment that is free from harassing or disruptive activity.

Definition of Sexual harassment as defined by the EEOC:

“Unwelcomed sexual advances, request for sexual favors, and other verbal or physical conduct of a sexual nature constitute sexual harassment when this conduct explicitly or implicitly affects an individual’s employment, unreasonably interferes with an individual’s work performance, or creates an intimidating, hostile, or offensive work environment.”¹

All other forms of harassment are unacceptable and include harassment based on race, color, national origin, religion, disability, pregnancy, age, military status, or sex. Such harassment has the purpose or effect of interfering with an employee’s work performance or creating an intimidating, hostile, or offensive working environment. This includes, but is not limited to:

- Verbal conduct such as epithets, derogatory comments, slurs, or unwanted sexual advances, invitation, or comments.
- Visual conduct such as derogatory posters, photography, cartoons, drawings, or gestures.
- Physical conduct such as unwanted touching, blocking normal movement, or interfering with work directed at you because of your sex or any other protected basis.
- Threats or demands to submit to sexual requests to keep your job or avoid some other loss, and offers of job benefits in return for sexual favors (This is known as “Quid Pro Quo”).
- Retaliation for opposing, reporting, or threatening to report harassment, or for participating in an investigation, proceeding, or hearing conducted by an investigating agency.
- Prohibited harassment is not necessarily limited to the loss of employment or some other economic benefit. Prohibited harassment that impairs your working ability or emotional well-being at work violates this policy.

¹ 29 CFR1604.11 (a)

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 4: ANTI-HARASSMENT AND HOSTILE-FREE WORK ENVIRONMENT

All employees share the responsibility of immediately reporting discrimination, including sexual harassment, to their manager/team leader, section/division director, or the Human Resource Manager. Except for the victim of sexual harassment, failure to report such conduct may result in disciplinary action up to and including immediate termination.

4.1 SEXUAL HARASSMENT AND ANTI-DISCRIMINATION TRAINING

All employees and supervisors shall receive Employment Discrimination training. Employees shall receive training no later than thirty (30) days after employment and supplemental training every two (2) years thereafter. Each employee is required to sign an acknowledgement verifying the completion of the training, which will be filed in the employee's personnel file.

4.2 COMPLAINT PROCEDURE

Employees who believe they have been subjected to sexual harassment or who have witnessed other employees being subjected to sexual harassment should follow the procedures below.

1. Report the complaint immediately to the employee's manager/team leader. Proceed to Step 2 if (a) for any reason you are uncomfortable approaching this person and do not wish to do so; (b) you file a complaint and no immediate action is taken, or (c) you are not satisfied with the action taken in response to your complaint.
2. Report the complaint to your section director. Proceed to Step 3 if (a) for any reason you are uncomfortable approaching this person and do not wish to do so, (b) you file a complaint and no immediate action taken, or (c) you are not satisfied with the action taken in response to your complaint.
3. Report the complaint to your division director. Proceed to Step 4 if (a) for any reason you are uncomfortable approaching this person and do not wish to do so, (b) you file a complaint and no immediate action taken, or (c) you are not satisfied with the action taken in response to your complaint.
4. Report the complaint to the Human Resources Manager.
5. The Human Resources Manager shall notify the General Counsel. The General Counsel shall immediately conduct an investigation of the allegations. A written report outlining the alleged actions and the investigation of such actions shall be forwarded to the Deputy Secretary of State for disposition.

4.3 ADDITIONAL ENFORCEMENT INFORMATION

The Equal Employment Opportunity Commission (EEOC) and the Texas Workforce Commission Civil Rights Division (TWCCRD) investigates complaints of harassment and discrimination.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 4: ANTI-HARASSMENT AND HOSTILE-FREE WORK ENVIRONMENT

4.4 DISCIPLINARY ACTION

If, after proper investigation, an employee has violated Section 4.0 above, the employee will be subject to immediate disciplinary action. Based upon the severity of the offense, disciplinary action may consist of training, counseling, a written reprimand, suspension without pay, demotion, salary reduction, or termination of employment.

4.5 CONFIDENTIALITY

Efforts shall be made to maintain confidentiality; therefore, disclosure of information relating to the complaint and investigation may be made only to the parties involved and other persons necessary to the investigation. Any employee who acquires knowledge of an investigation is to keep such information confidential

4.6 FALSE ACCUSATIONS

A deliberate false accusation by any complainant will result in appropriate disciplinary action against the complainant. False accusations will be determined by a third party using documented evidence showing the falsity of the complaint.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 5: EMPLOYMENT RECRUITMENT AND SELECTION

5.0 EMPLOYMENT “AT WILL” AND “RIGHT TO WORK”

Unless explicitly exempted by written contract, statute, or policy, all employees of the Agency are employed “at will” and, as such, are free to terminate their employment at any time with or without reason. The Agency likewise retains the right to determine that continued employment of an employee is not in its best interest. Furthermore, nothing in this Manual or any of its amendments, any statement made by supervisory personnel, either verbal or written, or any benefit program is intended to be nor should be construed as being a contract or guaranty of employment between the Agency and any employee. Any salary figures stated to an employee in annual or monthly terms are stated for the sake of convenience or to facilitate comparisons and are not intended to guarantee employment for any period of time.

All employees have a “right to work.” Employees cannot be denied public employment as a result of joining or not joining a labor union.

5.1 EMPLOYMENT RECRUITMENT AND SELECTION POLICY OBJECTIVES

The recruitment and selection procedures are based on three policy objectives:

- Selection based solely on objective, job-related criteria that can be consistently applied and quantifiably measured as to all classes of job applicants;
- Workforce diversity with an equitable distribution within all job classifications for all classes covered by anti-discrimination laws; and
- An employee selection plan solidly predicated on sound statutory and constitutional principles, as well as judicial interpretations that promote the elimination of unlawful discrimination.

5.2 RECRUITMENT AND SELECTION PROCEDURES.

The HRD will review all recruitment and selection procedures to ensure compliance with Agency policy and to ensure consistency. All personnel decisions, policies, procedures, and requirements shall be objective, job related, and measurable. Objective is defined as being concrete and observable as opposed to being subjective or using personal judgment. Applications, resumes, transcripts, letters of reference, and other similar documents submitted by applicants hired and not hired will be retained in accordance with the Texas State Records Retention Schedule.

The HRD shall maintain a comprehensive list of recruitment sources, including organizations representing minorities, women, and disabled persons. All sources on this recruitment list shall be sent a copy of the job posting, except when the vacancy is to be filled by promotion, re-employment of former employees, or transfer of current employees.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 5: EMPLOYMENT RECRUITMENT AND SELECTION

Applicants must submit The State of Texas Application for Employment. Applications are retained for a period of two (2) years.

5.3 PROCESS FOR RECRUITING AND SELECTING AN APPLICANT

The HRD publishes a Recruitment Notice only after the posting has been approved by the Secretary of State or the Deputy Secretary of State. A director may then direct the HRD to publish the notice either internally or externally after such approval has been obtained.

HRD Notifies Agency employees of the job vacancies posted on the intranet. All internal recruitment notices will remain posted for a minimum of three working days. If a recruitment notice is published internally and no one is selected to fill the position, the notice is then published publically. Recruitment Notices are provided to the following organizations:

- The Texas Workforce Commission via WorkInTexas.com;
- Established contact groups representing minorities, women, disabled, or older workers at state and local levels; and
- Appropriate educational institutions at state and local levels.

5.4 PROCESS FOR APPROVAL OF JOB POSTINGS

The request for all approved recruitment notices should include the following:

- **Job Description.** List all tasks that take at least 10% of the position's time. Be specific on responsibilities including reports due, number of persons supervised, and deadlines. Indicate qualifications. The job description should not contain any requirements that are not job related.
- **Job Qualifications.** Do not add any new tasks or responsibilities not included in the job description. Specific minimum qualifications, acceptable alternatives, and preferred qualifications should be included in the recruitment notice. Minimum job qualifications must incorporate education and experience. These two criteria must be job related and not have a statistically measurable disproportionate impact on covered classes included in laws prohibiting employment discrimination (race, color, sex, national origin, religion, age, mental or physical disabilities, and military status).

Preferred qualifications are the experience and education desired to accomplish the tasks and responsibilities of the position. Preferred qualifications, when used, will remain secondary in focus in selection and must be justified on the basis of business necessity or legitimate business objectives. Preferred qualifications shall be listed on the job posting under a separate heading entitled "Preferred Qualifications."

- **Job Testing.** All tests administered to applicants must be job related. General job-related tests will be administered and graded by the HRD. Job-specific tests may be

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 5: EMPLOYMENT RECRUITMENT AND SELECTION

administered by the HRD or the division/section having the vacancy and graded within the relevant division/section. Each test will become a permanent part of the application for employment.

- **Interview Questions.** The questions must be objective and job related and must measure an applicant's knowledge of the tasks listed in the job description. All applicants must be asked the same questions. The interviewer must keep notes of each applicant's answers. Interviews must be confined to the applicant's responses to job-related questions. Such questions are to focus exclusively on the applicant's professional and technical ability or knowledge to perform the duties of the job.
- **Applicant Rating Log.** The applicant rating log should list all predetermined selection criteria for the position. Each criterion must be given a value. All applicants should be listed on the applicant rating log.

The division/section director shall send to the HRD the job description, applicant rating log, interview questions, and any job-specific tests to be administered by the division/section. After the HRD reviews the job description and selection criteria to ensure compliance with Agency policy, the Human Resources Manager will forward the Personnel Action Request (PAR) to the Director of Administrative Services Division to confirm requisite funds are available for the requested action. The PAR will then be sent to the Deputy Secretary of State for approval.

5.5 EVALUATION OF EMPLOYMENT APPLICATIONS

All applications shall be evaluated based on predetermined selection criteria developed for the position. The selection criteria shall be based upon job tasks, experience and qualifications as set forth in the job description. Each criterion must be directly related to the job description and each criterion must be given a numerical value. Each application shall be screened using an applicant rating log. The applicant rating log is to be based on quantifiable job-related experience, tasks, and qualifications as set forth in the job description. As applications are evaluated, each applicant's name should be listed on the applicant rating log and numerical values determined for each selection criterion. With respect to promotion of current employees, the applicant rating log may include job performance evaluations and length of service with the Agency in addition to the other criteria established for the position. Applicants are to be ranked on the basis of their cumulative scores. The applicants in the highest numerical cluster shall be interviewed. As an alternative, the top five (5) applicants could be selected for interviews.

5.6 APPLICANT INTERVIEWS

After completing the interviews, the interviewer shall record on the applicant rating log any points received by each applicant for responses to interview questions and applicable job-specific tests. At least one job reference shall be obtained on the selected applicant and will be included with the selection criteria information forwarded to the HRD for review.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 5: EMPLOYMENT RECRUITMENT AND SELECTION

5.7 EMPLOYMENT PREFERENCES

An individual who qualifies for an employment preference as a veteran or former foster child is entitled to a preference in employment over other applicants for the same position who are otherwise equally qualified.

All applicants will receive veteran's preference, if entitled, until forty percent (40%) of the Agency's workforce comprises those that are entitled to said preference. Once 40% of the Agency's workforce is persons qualifying for the preference, the preference need not be given.

5.8 QUALIFICATIONS FOR VETERAN'S PREFERENCE

An individual qualifying for the Veterans Preference must fulfill the following criteria:

- The Veteran served in the military for not less than ninety (90) consecutive days during a national emergency declared in accordance with federal law or was discharged from military "service for an established service-connected disability."
- The Veteran has an Honorable Discharge; and
- The Veteran is competent.

Surviving spouses who have not remarried and orphans qualify for the veteran's preference under the following circumstances:

- The veteran was killed on active duty;
- The veteran served in the military for no less than ninety (90) consecutive days during a national emergency in accordance with federal law; and
- The spouse or orphan is competent.

5.9 QUALIFICATIONS FOR FOSTER YOUTH PREFERENCE

An individual qualifies for foster youth preference must fulfill the following criteria:

- The individual was under the permanent managing conservatorship of the Department of Family and Protective Services on the day preceding the individual's 18th birthday.
- The individual is 25 years of age or younger.

5.10 APPLICANTS WITH A CRIMINAL RECORD

The Agency's policy regarding the hiring of persons with a criminal record is intended, among other things, to provide a crime-free work environment and to produce a law-abiding workforce. (The term "criminal record" in this context includes both convictions and deferred adjudication.)

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 5: EMPLOYMENT RECRUITMENT AND SELECTION

If an applicant is otherwise qualified for the position, a criminal record will not automatically disqualify the applicant. However, the following factors will determine whether to consider the applicant for employment:

- The specific duties of the position.
- The number of offenses committed by the individual.
- The nature and seriousness of each offense.
- The length of time between the offense and the employment decision.
- The efforts by the individual at rehabilitation.
- The accuracy of the information on the applicant's employment application.
- Any other relevant factors.

5.11 FINAL SELECTION

Subject to the Nepotism policy (Section 2.13), the applicant receiving the highest cumulative score based on the established selection criteria shall be selected to fill the position. The section/division director notifies the Human Resources Manager of final selection. All information used for the selection of the applicant, including information for applicants not hired, must be submitted to the HRD. The HRD will review the information to ensure compliance with Agency policy and consistency. The HRD will conduct employment reference checks and criminal history background checks on the selected applicant. Additionally, HRD will verify the Selective Service System registration status on males ages 18-25.

An individual who is not a citizen of this country is protected from discrimination under the provisions of federal law and the Texas Labor Code. It is unlawful to discriminate on the basis of citizenship or "intending citizen" status. However, federal law prohibits the Agency from knowingly hiring an individual who is not authorized to work in this country. To ensure compliance, the Agency is required to complete Form I-9, Employment Eligibility Verification, upon hiring a person. This form must be completed within three business days of the hire.

The HRD will complete a PAR listing the name of the applicant, Classification Title, Class Number, Salary Group, monthly salary, and position number. The PAR (and the results of the criminal history check if a conviction or deferred adjudication is discovered) will be forwarded to the Secretary of State or the Deputy Secretary of State for final approval. With the exception of the staff of the Executive Division, only the HRD may extend an offer of employment to an applicant. If an applicant accepts or declines the offer of employment, the HRD will notify the hiring director and/or team leader.

The manner of recruitment and selection of employees for the Executive Division is within the discretion of the Secretary of State or the Deputy Secretary of State.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 5: EMPLOYMENT RECRUITMENT AND SELECTION

5.12 NEW EMPLOYEE ORIENTATION

Within thirty days of hire all new employees will be advised of employee benefits and responsibilities, the Agency’s responsibility in providing a safe and secure workplace, and the general rules regarding Agency policy. The orientation covers the following topics:

- Agency Organization
- Working hours
- Use of state property
- Workers’ Compensation
- Safety program
- Employment Discrimination and Sexual Harassment
- Parking
- Payroll
- Overtime
- Compensatory time
- Deferred Compensation
- Insurance
- TexFlex
- Timesheets
- Types of leave
- Leave accrual

The manager/team leader must complete and return the Orientation Checklist to the HRD within five work days after the date of hire. Managers/team leaders are responsible for providing an orientation session regarding the policies and procedures applicable to their respective section.

5.13 INITIAL TRIAL PERIOD OF EMPLOYMENT

New or returning employees are subject to an initial trial period of employment of 180 days. During this initial period, job performance, attendance, and conduct are reviewed and evaluated. If an employee’s employment is terminated during or at the conclusion of this initial period, the employee may not take advantage of the agency’s disciplinary and grievance policies.

Notwithstanding any of the above, during this initial trial period, a new employee’s employment can be terminated at any time for any reason. The existence of an initial trial period of employment in no way affects the “at-will” status of employees during their employment.

Upon satisfactory completion of the initial trial period of employment, the employee will no longer be in the trial period and will have the right to utilize the agency’s disciplinary and grievance process.

New or returning employees shall sign an acknowledgment that they are subject to this initial trial period.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

**SECTION 6: FAIR LABOR STANDARDS ACT (FLSA) AND STATE AND
HOLIDAY COMPENSATORY TIME**

6.0 GENERAL

The Fair Labor Standards Act (FLSA) establishes minimum wage, overtime pay, recordkeeping, and child labor standards affecting full-time and part-time workers in the private sector and in federal, state, and local governments. The U.S. Department of Labor's (DOL) Wage and Hour Division (WHD) is responsible for providing guidance on and enforcement of the FLSA. Additional information about the FLSA can be found at www.dol.gov/esa/whd.

6.1 DETERMINATION OF FLSA STATUS

The agency determines FLSA status (Exempt or Nonexempt) using the Short Test for FLSA Compliance Form issued by the Department of Labor.

6.2 DEFINITIONS

- “Work week” consists of the first forty (40) hours the employee is actually on the job during the period beginning 12:00 a.m. Sunday and ending midnight Saturday.
- “Paid week” consists of forty (40) compensated hours, not all of which the employee has actually worked because the employee is on paid leave (such as annual leave, sick leave, compensatory leave, overtime leave, holiday, jury duty, etc).
- “FLSA-exempt employees” are employees not subject to the overtime provisions of the FLSA.
- “FLSA-non-exempt employees” are employees subject to the overtime provisions of the FLSA.
- “Overtime worked” consists of hours worked by a non-exempt employee in excess of a “work week” (that is, where the employee has actually worked forty (40) hours and then works additional time).
- “State compensatory time” for a non-exempt employee consists of those hours worked in excess of a “paid week” (that is, where the employee is compensated for forty (40) hours, not all of which he/she has actually worked) that when added to the number of hours actually worked during the week, does not cause the resulting total number of actual hours to exceed forty (40).
- “FLSA-compensatory time” for an exempt employee consists of hours worked in excess of either a “paid week” or a “work week.”

6.3 EMPLOYEES NOT EXEMPT FROM THE FLSA

Non-exempt employees are covered by the FLSA and are entitled to the benefits of the act as regards time worked in excess of a forty (40) hour work week. Employees must use accrued overtime before using annual leave. See **ANNUAL LEAVE**. Employees will receive payment of accrued overtime upon termination of employment.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

**SECTION 6: FAIR LABOR STANDARDS ACT (FLSA) AND STATE AND
HOLIDAY COMPENSATORY TIME**

Non-exempt employees who receive prior approval from their section/division directors to work hours in excess of forty (40) hours in a workweek are entitled to compensation for the excess hours either by:

- Taking FLSA-compensatory time off at the rate of 1.5 hours off for each hour of overtime worked; or
- Receiving pay for the overtime worked at a rate equal to 1.5 times the employee's regular rate of pay.

The section/division director shall determine which of the above compensation methods is appropriate subject to the exception noted below. Any FLSA-compensatory time taken under this subsection shall be subject to the provisions for state compensatory time outlined below.

A non-exempt employee may accrue a maximum of 160 hours of overtime that may be taken as compensatory time off at 1.5 hours for each hour or compensated with extra pay at 1.5 times the employee's regular rate of pay at the discretion of the section/division director.

Exception: However, if an employee logs more than one hundred and sixty (160) hours of overtime, those hours over 160 must be compensated with extra pay. In addition, an employee who receives a pay increase of any type may be required to exhaust all accrued overtime or receive payment for all accrued overtime before the effective date of the pay increase. The selection of payment method will be at the discretion of the section/division director.

Policy for Recording FLSA Overtime Worked/Taken – All overtime hours worked or taken should be recorded on the timesheet as exact minutes worked or taken during the month.

6.4 EMPLOYEES EXEMPT FROM FLSA OVERTIME PROVISIONS

Subject to the exceptions provided below, an FLSA-exempt employee shall receive full salary for any week in which work is performed without regard to the days and number of hours worked. This policy is also subject to the following exceptions, as well as the general rule that an employee need not be paid for any workweek in which the employee performs no work.

Deductions may be made when an employee is absent from work for a full day or more for personal reasons other than sickness or accident. However, deductions may not be made for absences caused by jury duty, attendance as a witness at a judicial action, or temporary military leave.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

**SECTION 6: FAIR LABOR STANDARDS ACT (FLSA) AND STATE AND
HOLIDAY COMPENSATORY TIME**

Deductions may be made for absences of a day or more occasioned by sickness or disability (including workers' compensation accidents) if the deduction is made after exhaustion of sick leave or workers' compensation benefits.

Deductions may be made for penalties imposed for infractions of significant safety rules relating to prevention of serious danger to the workplace or other employees.

An FLSA-exempt employee's pay may also be reduced for absences for personal reasons or because of illness or injury of less than one (1) work day when accrued leave is not used by the employee because:

- Permission for its use has not been sought or has been denied;
- Accrued leave has been exhausted; or
- The employee chooses to use leave without pay. See **LEAVE WITHOUT PAY**.

6.5 STATE COMPENSATORY TIME

Employees exempt from the overtime provisions of the FLSA are entitled to take state compensatory time off at the rate of one (1) hour off for each hour worked in excess of a forty (40) hour work week or paid week.

Employees may accrue state compensatory time for work performed at any location other than the employee's regular place of employment or duty point with advance approval from the Secretary of State or Deputy Secretary of State.²

The Secretary of State is not entitled to accrue state compensatory time. An employee in Salary Groups B25 and above is not entitled to accrue state compensatory time except when working on a holiday, an election day, or during election night returns; when serving as an election inspector; when working because of legislative necessity; or for making extraordinary work efforts approved by the section/division director. Prior approval by the section/division director of the employee is required. Division directors must receive approval from the Secretary of State/ Deputy Secretary of State to accrue state compensatory time.

All state compensatory time worked must be approved in advance by the section/division director.

State compensatory time must be taken during the twelve (12) month period following the week during which the state compensatory time was worked and may not be carried forward past the end of the twelve (12) month period. Under no circumstances shall employees be paid for any unused state compensatory time earned unless work performed

² SB 2298, 81st Legislature, R.S.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

**SECTION 6: FAIR LABOR STANDARDS ACT (FLSA) AND STATE AND
HOLIDAY COMPENSATORY TIME**

was directly related to a disaster or emergency declared by the Governor or his/his designee.

If an employee submits a written request to use accrued compensatory time no later than the 90th day before the date on which the accrued compensatory time will lapse, the section/division director shall approve in writing the employee's request or provide the employee with an alternate date on which the employee may use the compensatory time. The agency is encouraged to reasonably accommodate the employee's use of accrued compensatory time.

All employees will receive annually the State's policy on compensatory time.

6.6 HOLIDAY COMPENSATORY TIME

An employee who must work on a designated national or state holiday will be allowed holiday compensatory time off during the 12-month period following the date of the holiday if the state employee is entitled to a paid day off from working for a state agency on the holiday. An employee is required to give reasonable advance notice when taking holiday compensatory time; however, an employee does not have to specify the reason for the request. Holiday compensatory time is earned at the straight time rate of an employee's hourly rate.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 7: SALARY ADMINISTRATION AND EMPLOYEE COMPENSATION

7.0 GENERAL INFORMATION

The Position Classification Plan includes three salary schedules:

- Schedule A for paraprofessional, administrative support, protective service, maintenance, service and technical positions;
- Schedule B for primarily professional and managerial positions; and
- Schedule C for specific law enforcement positions certified by the Commission on Law Enforcement Officer Standards and Education (CLEOSE).

7.1 NEW HIRE SALARY RATE

The Secretary of State or Deputy Secretary of State may determine, at the time of initial employment (to include rehires and interagency transfers) the salary increment or rate within the applicable salary schedule for employees classified under the Position Classification Act.

7.5 PROMOTION

There are two methods by which employees may be promoted.

- Vacant positions – An employee may be promoted by filling a vacant position that is in a higher salary group than his/her present job classification.
- Change in Duty Assignment and Responsibilities – An employee may be promoted if his/her present duty assignments change to those of a classification in a higher salary group.

Promotion Eligibility Criteria

Employees are not eligible for a promotion until they have been employed for six (6) continuous months with the Agency. Qualified employees who have consistent high job performance but have not been employed for six (6) consecutive months may be selected to fill vacant position within their section. In these instances, the division/section director must complete and forward to the HRD a special evaluation, that reflects the consistent high job performance.

Employees are not eligible to apply for vacant positions in another section or division, irrespective of whether their selection would mean a promotion, until they have been employed for six (6) continuous months with the Agency.

Employees who were previously employed by the Agency and are rehired must meet the six (6) continuous month employment requirement starting from the rehire date. Previous employment time will not be counted toward the requisite continuous employment period.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 7: SALARY ADMINISTRATION AND EMPLOYEE COMPENSATION

Promotions, by either of the two previously stated methods, may be granted anytime after an employee has been employed by the Agency for six (6) continuous months regardless of when the employee received his/her last promotion.

The employee's overall performance must be considered for all promotions. The employee must have demonstrated that he/she is capable of handling additional responsibilities and performing higher levels of work. The employee's most recent Employee Appraisal must reflect consistent high job performance.

Promotion Pay Rate

Promoted employees may receive the maximum rate for the salary range to which they are promoted.

7.6 DEMOTION

A demotion is a change in job classification that provides a lower minimum salary rate. The salary of a demoted employee on Salary Schedule A will be reduced at least \$30 a month for full-time employees. The salary of a demoted employee on Salary Schedule B will be reduced by at least 3.4 percent to a level below the employee's current salary.

7.7 SALARY REDUCTION FOR DISCIPLINARY REASONS

The Secretary of State/Deputy Secretary of State may reduce a classified employee's pay for disciplinary reasons if warranted by the employee's performance. The reduced salary cannot be lower than the minimum rate of the employee's current salary group. Pay may be restored to any rate within the same salary group, up to and including the employee's prior rate, as performance improves without accounting for the increase as a merit increase.

7.6 REALLOCATION

Classified employees whose positions are reallocated to higher salary groups will receive the minimum rates in the higher salary groups or the salaries they would receive without the reallocation, whichever are higher. Salaries of employees may not be increased more than 6.6 percent for the purpose of maintaining desirable salary relationships among employees in the affected positions.

Employees whose positions are reallocated to a lower salary group will receive the salaries they would have received had the positions not be reallocated. However, employee's salaries should not exceed the maximum rates for the lower salary groups.

7.9 RECLASSIFICATION

Reclassification is defined as a change in the classification of a position based on the actual duties performed by an employee. It does not refer to a change in an employee's duty assignment or changes to the Classification Plan. Annually, the Agency reviews job assignments to ensure that employees are classified properly.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 7: SALARY ADMINISTRATION AND EMPLOYEE COMPENSATION

7.10 MERIT INCREASE/ONE-TIME MERIT

Merit increases and One-time Merits are for employees whose job performance and productivity are consistently above that required or normally expected. Merit increases are meant to recognize outstanding service on the job and result in a higher rate of pay for doing the same job.

The eligibility criteria for Merit Increases/One-Time Merits is as follows:

- Employment for six (6) continuous months from the date of hire/rehire with the Agency prior to the award, excluding any full calendar months of leave without pay.
- Employees may not receive a merit salary increase or a one-time merit payment unless six (6) months have elapsed since their last merit increase, one-time merit payment, promotion, demotion or enhanced compensation award.
- Employee's most recent Employee Appraisal must reflect consistent high job performance.

Justifications must satisfy the following criteria to substantiate all merit increases and one-time merits.

- The employee must have contributed in some significant manner (as determined by his/her director) to achieving the goals of the employee's section/division or of the Agency and/or performed an act of achievement that brings distinction to the section/division or Agency; and
- The employee must have been employed in a classified position for at least six (6) consecutive months with the Agency and have had a job performance record which reflects performance that consistently exceeds that which is normally expected. These achievements must be documented on the employee's most recent employee performance evaluation.

7.11 MERIT SALARY RATE

For classified employees on Salary Schedule A or B, a merit increase involves an increase in an employee's salary within the same salary group. There is no minimum or maximum amount specified for the size of either merit salary increases or one-time merit payments.

7.12 EQUITY ADJUSTMENTS

The agency has the authority to adjust the salary rate of an employee whose position is classified under the Position Classification Plan to any rate within the employee's salary group as necessary. The equity adjustment is to be used to maintain desirable salary relationships between and among agency employees and employees who hold similar positions in the relevant labor market.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 7: SALARY ADMINISTRATION AND EMPLOYEE COMPENSATION

The agency will consider education, skills, related work experience, length of service, and job performance of employees when comparing desirable salary relationships between employees in the agency and similar employees in relevant job markets.

An employee may receive an equity adjustment only if he/she has been employed by the agency in the current position for six months while maintaining a satisfactory level of performance. Employees may not receive more than one equity adjustment per fiscal year and adjustments can be considered during the annual classification review.

7.13 ENHANCED COMPENSATION AWARD

Article IX, Section 6.13 (d) of the 2010-2011 General Appropriations Act, in part, states the following: *“To further foster, support, and reward outstanding performance, ongoing productivity improvements and innovative improvement programs, and to retain key high performing employees, qualified state agencies may expend amounts necessary from funds appropriated in this Act for the purposes of enhancing compensation for employees who directly contributed to such improvements.”*

The Agency is authorized to compensate its employees under the legislative provisions as stated above. The Agency’s intent is to establish an Enhanced Compensation Program that will reward outstanding performers, employees directly involved with ongoing productivity improvements, which impact the Agency’s key performance measures, and if necessary to retain key high-performing employees in these areas. Enhanced compensation awards shall not exceed 6.6 percent of employee’s annual base pay.

Eligibility Criteria

To be eligible for the Enhanced Compensation Award Program, the Agency must:

1. Achieve or exceed targets for 60 percent of the established key performance measures;
2. Have an unqualified certification of at least 70 percent of its performance measures as shown by its most recent certification review by the State Auditor’s Office;
3. File a report with the Comptroller of Public Accounts (CPA), Legislative Budget Board (LBB), Governor’s Office of Budget and Planning (GOBP), House Appropriations Committee, and Senate Finance Committee describing the success of the innovative program and criteria used to assess the improvements;
4. Sixty days prior to implementation, file a report with the CPA, LBB, GOBP, House Appropriations Committee, and Senate Finance Committee describing in detail how the Agency intends to use this flexibility to further the goals of the Agency.

In addition divisions/sections must:

1. Have organizational performance measures approved by the Secretary of State. These performance measures will be LBB performance measures or be in addition to LBB performance measures where LBB measures do not exist, and

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 7: SALARY ADMINISTRATION AND EMPLOYEE COMPENSATION

2. Ensure that there is sufficient evidence to determine proper control and verification of the validity of the measures being tracked.

Only those areas which accurately document and report performance measures, and which exceed targets are eligible.

Application Procedure

1. Employees must be classified employees in Salary Group B16 or below, and be directly involved in meeting performance measures as outlined with the LBB.
2. The responsible section/division director must prepare a memorandum detailing the type of enhanced compensation being recommended and describe in detail the justification for the award being recommended.
3. The employee's job performance must have been generally documented as "exceeding" in either the employee's current performance appraisal or in a memorandum that documents accomplishments, degree of difficulty of assignment and/or level of supervision required, and with no "Needs Improvement" or unsatisfactory rating in any performance category.
4. Specific, verifiable performance documentation must be available to substantiate any compensation under this program.
5. The Secretary of State or Deputy Secretary of State will review and approve all Enhanced Compensation Awards.

7.14 LATERAL TRANSFERS

A lateral transfer is a change in duty assignment of an employee that moves the employee to another job class in the same salary group.

7.15 TEMPORARY ASSIGNMENT

Employees may be temporarily assigned to other duties for a period not to exceed six months. During that time, employees will receive at least the same amount of pay he or she received prior to the assignment. Employees will not be temporarily assigned to a position with a new lower minimum salary rate. Such assignments will not exceed 6 months in a 12-month period. During the temporary assignment, the employee will not receive merit increase, promotion, or demotion

7.16 BASE SALARY

- The monthly base salary for full-time employees is the rate for the classified position.
- The monthly base salary for part-time employees is a percentage of the full-time rate for the classified position. The percentage is calculated as the ratio of actual time worked per day to a normal eight (8) hour day. For example, an employee who works four (4) hours of the normal eight (8) hour working day is paid fifty percent (50%) of the full-time rate for that position.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 7: SALARY ADMINISTRATION AND EMPLOYEE COMPENSATION

- The hourly base salary shall be calculated using 2,060 hours as the average number of work hours in a year (52 weeks multiplied by 40 hours per week) and 173.33 hours as the average number of hours in a month (2,060 hours divided by 12 months).
- Base Salary for Partial Month – Employees employed after the first workday of a month or those terminating employment or placed on leave without pay during a month shall receive a partial salary payment for the partial month’s work. This payment is determined by a fraction whose numerator is the actual number of days or hours worked, and whose denominator is the total number of workdays (including holidays) or hours in the particular month.

7.17 LONGEVITY PAY

Regular full-time and line item/exempt employees not on Leave Without Pay on the first workday of each month are entitled to longevity pay of \$20.00 for every two years of service credit. For employees returning from military leaves of absence, please see policy on Leave Without Pay in Section 5.

Table 1 shows the amount of Longevity Pay for each two years of service credit.

Table 1.

Years of Service	Monthly Longevity Pay
Less than 2	\$0
Less than 4	\$20
Less than 6	\$40
Less than 8	\$60
Less than 10	\$80
Less than 12	\$100
Less than 14	\$120
Less than 16	\$140
Less than 18	\$160
Less than 20	\$180
Less than 22	\$200
Less than 24	\$220
Less than 26	\$240
Less than 28	\$260
Less than 30	\$280
Less than 32	\$300
Less than 34	\$320
Less than 36	\$340
Less than 38	\$360
Less than 40	\$380
Less than 42	\$400
Greater than 42	\$420

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 7: SALARY ADMINISTRATION AND EMPLOYEE COMPENSATION

Longevity Pay for Return-to-Work Retirees

An employee who retired from state employment before June 1, 2005, and who returned to state employment before September 1, 2005, is entitled to receive longevity pay. The monthly amount of longevity pay the employee is entitled to receive equals the amount of longevity pay that the employee was entitled to receive immediately before September 1, 2005. An employee who retired from state employment before June 1, 2005, and who returned to state employment on or after September 1, 2005, is not entitled to receive longevity pay.

7.18 BENEFIT REPLACEMENT PAY (BRP)

Employees who, on August 31, 1995, had their social security contributions paid by the state under the authorization of the previous law are entitled to BRP in accordance with Section 659.122 of the Texas Government Code. Salary or wages paid to eligible state employees after December 31, 1995, shall include BRP.

Benefit Replacement Pay is equal to the sum of (1) 5.65 percent of the **Federal Insurance Contributions Act (FICA)** covered wages (up to the level of \$16,500) earned by the employee during the pay period and (2) an amount equal to the additional retirement contribution paid by the employee because of the BRP. The amount paid on behalf of eligible employees, not including the additional retirement contribution, may not exceed \$965.25 each calendar year.

Employees who are entitled to receive the maximum amount of BRP may during the calendar year opt to be paid in equal installments known as “leveling.” However, if an employee elects to level and later terminates employment before the end of the calendar year, they will not be paid the difference between the BRP paid and the amount they would have received had they not chosen to level. Also, eligible employees who leave state employment after August 31, 1995, for at least thirty (30) consecutive days before returning to state employment are not eligible to receive BRP. Effective September 1, 2005, eligible employees who retired from state employment on or after June 1, 2005, are **not** eligible to receive BRP.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 8: PAYROLL AND PERSONNEL REPORTING

8.0 PAYDAY

Payday is on the first business day of the month. The only exceptions to an employee receiving pay on the first business day of the month is when an employee is placed on a supplemental payroll because the employee was hired or was on Leave Without Pay (LWP) after submission of the regular payroll.

8.1 PAYROLL ADJUSTMENT FOR EMPLOYEES ON LEAVE WITHOUT PAY

The Payroll Accountant will adjust the pay for an employee on LWP for the number of hours that is less than a full pay period.

- An employee who is on LWP and returns to work **before** the 15th day of the month will receive a partial payment on payday that reflects payment for the preceding pay period minus the number of hours of LWP.
- An employee who is on LWP **after** the 15th of the month shall receive full payment on payday. During the next pay period, the employee's payment on payday will reflect an adjustment for the number of hours of LWP from the previous pay period.

Any LWP that includes a full pay period shall be considered "extended leave without pay." An employee's regular payment will be canceled upon receipt of notification from the section/division director notifying the HRD of the extended leave without pay. A supplemental payment shall be issued to the employee for hours worked prior to being placed on LWP, if applicable.

Exception: Notification received during the last five (5) working days of a month will NOT cause an employee's payment to be canceled unless a termination notice has been given or there are other concerns about an employee's intention to return to work.

8.2 METHOD OF RECEIPT OF PAYMENT

Direct Deposit - Employees may have their warrants (a/k/a paychecks) deposited into their bank accounts. Employees must submit a Form 74-158, EMPLOYEE DIRECT DEPOSIT AUTHORIZATION to the HRD. Employees with direct deposit must access the Employee Information System (EIS) to obtain their Statement of Earnings.

TexPayCard - Employees may have their warrants deposited onto a prepaid card. Employees must submit a Form 74-224, EMPLOYEE PAYCARD AUTHORIZATION to the HRD.

Employee Receipt - Warrants, with the exception of those directly deposited, are distributed directly to employees on payday. If a warrant is issued on a supplemental payroll, the warrant is distributed to the employee when it is received from the Comptroller of Public Accounts. Upon receipt of a written authorization from an

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 8: PAYROLL AND PERSONNEL REPORTING

employee, the Financial Management Section will deliver or release the employee's warrant(s) to a designated recipient.

8.3 DEDUCTIONS FROM GROSS PAY

No deduction may be made from an employee's salary unless required by federal law or authorized by the Texas Legislature.

Mandatory Deductions Required by Federal Law or State Statute

- Federal Income Tax – Federal income tax withholding will be deducted from an employee's gross pay. The amount of deduction is based on taxable salary and on information on Form W-4 and Form W-5.
- Social Security Tax - Deductions under the Federal Insurance Contributions Act (FICA), also known as social security tax. There are two types of deductions:
 - Old Age, Survivors, and Disability Insurance (OSDI) – Employees are subject to a deduction of 6.2 percent of pretax salary.
 - Medicare – Employees are subject to a deduction of 1.45 percent of pretax salary.
- Retirement Contributions – Employees are subject to a deduction of 6.5 percent of gross salary each month. (See **Retirement and Death Benefits 12.2**)
- Child Support Payments – A court may order any employer, including the Agency, to withhold child support payments from an employee's wages.
- Federal Tax Liens – The Secretary of State will deduct from an employee's salary the amount to be withheld pursuant to a Notice of Levy filed by the Internal Revenue Service (IRS). The employee may not receive any warrants until the IRS submits a Release of Levy/Release of Property from Levy to the Financial Management Section.

Voluntary Deductions Authorized by the Texas Legislature

- Insurance - Premiums for medical, dental, and optional insurance. (See **Employee Benefits Section 12**)
- Deferred Compensation Plans - Contributions to 401(k) and/or 457 Deferred Compensation accounts.
- Flexible Spending Accounts (FSA) - Employees may elect to pay eligible medical and daycare expenses with pretax dollars.
- State Employee Organizations, Credit Unions, and Charitable Organizations - An employee may authorize a deduction each pay period from salary for a membership fee in an eligible state employee organization, a payment to a credit union share account, or a contribution to an eligible charitable organization. Employees may contact the Payroll Accountant in the Financial Management Section for additional information.
- Texas Prepaid Higher Education Tuition Program - Certain prepaid tuition or college savings contracts can be paid through payroll deduction.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 9: GENERAL AND MISCELLANEOUS LEAVE

9.0 AUTHORIZATION FOR LEAVE

All leave taken, with certain exceptions, must be approved in advance by the employee's manager/team leader. Exceptions are for the following:

- Unforeseeable sick leave (e.g., other than prearranged medical or dental appointments); and
- Some emergency leave situations.

If an employee must be absent from duty because of an exception listed above, the employee must notify the manager/team leader at the earliest possible time. (Failure to notify may result in disciplinary action.)

If an employee takes leave before it is approved, and no exception applies, such leave is considered an unauthorized absence and may subject the employee to disciplinary action.

A No-Call/No-Show of three (or more) consecutive workdays will be considered job abandonment and will result in involuntary termination of employment. (**See Job Abandonment Section 17.**) A “**NO CALL NO SHOW**” is anytime an employee is absent from his/her scheduled shift and fails to notify his/her supervisor that he/she will not be at work OR that he/she is leaving work.

Employees must submit a timesheet to the HRD on the last business day of the month. The Secretary of State is exempt from the Position Classification Plan and may approve his/her own timesheet and leave (except for emergency leave, extended sick leave, or leave without pay).

Employees requesting leave for more than ten consecutive workdays will be required to receive approval from their section/division director and the Deputy Secretary of State/Secretary of State. Employees will request the leave by completing the Request and Authorization for Leave form. Once the leave has been approved by the section/division director, the form will be submitted to the Deputy Secretary of State/Secretary of State for approval.

9.1 LEAVE SUMMARY

The Leave Summary is a report that lists an employee's leave accruals and leave balances. It also contains messages notifying employees when they have to use annual leave and compensatory time to avoid losing the accrued time. Leave summaries are accessible from the Employee Information System (EIS).

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 9: GENERAL AND MISCELLANEOUS LEAVE

9.2 ANNUAL LEAVE

An employee employed for six (6) continuous months with the state is entitled to annual leave with pay each year. An employee earns annual leave beginning on the first day of employment with the state and each succeeding month thereafter, and terminating on the last day of duty. Employees who are on leave the first day of the month must return to duty before being eligible to use leave accrued for that month.

An employee who terminates state employment is entitled to payment of annual leave accrued, provided that the employee had been continuously employed with the state for at least six (6) months. However, if an employee terminates state employment and is re-employed within thirty (30) calendar days by another state agency that accrues annual leave, the employee's previously accrued but unused annual leave will be restored.

Employees may carry the net balance of unused accumulated annual leave from one fiscal year to the next but may not exceed the maximum cited in Table 2 below. The table below shows, for full-time employees, the rate of accrual of annual leave based on total state service credit and the maximum number of hours that may be carried forward each fiscal year. (The state's fiscal year begins on September 1st.) Part-time employees accrue annual leave on a proportionate basis. The maximum carryover will also be proportionate.

Table 2

Length of State Service (in years)	Monthly Rate of Accrual	Annual Hours of Accruals	Maximum Carryover*
Less than 2	8	96	180
Less than 5	9	108	244
Less than 10	10	120	268
Less than 15	11	132	292
Less than 20	13	156	340
Less than 25	15	180	388
Less than 30	17	204	436
Less than 35	19	228	484
Greater than or equal to 35	21	252	532

*Maximum carryover of hours that may be carried forward on September 1. Annual leave that exceeds the maximum carryover will be credited to the employee's sick leave balance at the end of the fiscal year.

Annual leave for employees who retired from state employment on or after June 1, 2005, will accrue annual leave based on the date of rehire. Return-to-work retirees are not required to re-establish the six-month continuous service requirement to use annual.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 9: GENERAL AND MISCELLANEOUS LEAVE

Employees must use accrued overtime before using annual leave.

9.3 SICK LEAVE

Sick leave entitlement shall be earned at the rate of eight (8) hours for each month or fraction of a month of full-time employment with the state. Sick leave for part-time employees is accrued on a proportionate basis. There is no limit to the amount of sick leave that may be accrued or carried forward from one fiscal year to the next. Sick leave accrues monthly beginning on the first day of employment and terminates on the last day of duty.

An employee may use sick leave when prevented from performing his/her job because of illness, injury, or pregnancy or confinement. Employees who are on leave on the first day of the month may not use sick leave accrued for that month until after a return to duty. An employee may also use sick leave if he/she needs to care for an immediate family member who is actually ill.

“Immediate family” is defined as individuals related by kinship, adoption, or marriage who live in the same household; foster children who reside in the same household; and minor children regardless of whether they live in the same household. Sick leave may be used only for a documented medical condition to care for immediate family members who do not reside in the same household. In this instance only, “immediate family” is interpreted as spouse, parent, or child.³

An employee who is the legal guardian of a child by court appointment may use sick leave to care for the child. Sick leave may be used for the adoption of a child under the age of three (3). An employee’s use of sick leave for family members not residing in the employee’s household is strictly limited to the time necessary to provide care and assistance to a spouse, child, or parent of the employee who needs such care and assistance as a direct result of a documented medical condition. In such cases an employee is required to complete and submit a Sick Leave Affidavit (See Appendix A).

If an employee must be absent from duty because of illness, the employee should notify a manager/team leader at the earliest practicable time. To be eligible for sick leave with pay during a continuous period of more than three (3) business days, an employee must send the Secretary of State Human Resource Department a Healthcare Provider’s Statement (See Appendix A) or an acceptable written statement of facts, if permitted by the Human Resources Manager for similarly situated employees, showing the cause or nature of the illness. An “acceptable” written statement of facts would be one, for example, that explains that the employee has a condition, such as the flu, so common, recognizable, and non-threatening that consulting a doctor for diagnosis or treatment

³ Texas Government Code, Section 661.202(e); and State Auditor’s Office Leave Interpretation Letter, No. 97-04 (1996)

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 9: GENERAL AND MISCELLANEOUS LEAVE

would be unnecessary. It is within the discretion of the Secretary of State/Deputy Secretary of State to require documentation concerning illnesses resulting in absences of three (3) working days or less. The Secretary of State delegates this authority to the section/division directors when leave records show a re-occurring leave pattern or other re-occurring leave during peak workloads.

In the case of a workers' compensation injury or illness, an employee may be eligible to participate in the Agency's Return to Work Program.

Employees who separate from state employment under a formal reduction in force are entitled to have their sick leave balances restored if they are re-employed by the state within 12 months.

Employees separated for reasons other than a formal reduction in force and re-employed by the same state agency may have their sick leave balances restored only if:

- The employee is re-employed by the same state agency or institution of higher education within 12 months after the end of the month in which the employee separates from state employment, and if there has been a break in employment with the State of at least 30 calendar days; or
- The employee is re-employed by a different state agency or institution of higher education within 12 months after the end of the month in which the employee separates from state employment.

9.4 SICK LEAVE POOL

Except for the Secretary of State, employees may apply for leave from the sick leave pool (Pool) for their own catastrophic injury or illness or for a member of their immediate family. Employees with a catastrophic injury or illness are eligible to apply to use the sick leave pool after exhausting all accrued leave. Employees must apply for and use the sick leave pool for which they are eligible prior to the application and use of any extended sick leave benefits.

A catastrophic illness or injury is defined by the Employees Retirement System as:

A severe condition or combination of conditions affecting the mental or physical health of the employee or the employee's immediate family that requires the services of a licensed practitioner for a prolonged period of time and that forces the employee to exhaust all leave time earned by that employee and to lose compensation from the state for the employee.

Generally, an injury or illness has to be considered life-threatening by a physician or licensed practitioner to be classified as "catastrophic."

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 9: GENERAL AND MISCELLANEOUS LEAVE

Examples of mental health conditions that may be considered catastrophic are major depression, bipolar disorder, schizophrenia, or other psychotic disorders.

Examples of physical health conditions that may be considered catastrophic are cancer, brain tumors, heart attacks, strokes, acquired immune deficiency syndrome, or cerebral aneurysms.

Examples of conditions not usually covered unless accompanied by a catastrophic condition or a complication considered to be life-threatening include gynecological problems and conditions, hysterectomies, gall bladder surgery, surgery for a herniated disk, carpal tunnel syndrome, allergies, bronchitis, most broken bones and orthopedic surgeries, angina, pregnancy and childbirth, and post-partum recovery.

“Licensed practitioner” means a “practitioner,” as defined in the Texas Insurance Code, who is practicing within the scope of his/her license.

“Immediate family” is defined as those individuals related by kinship, adoption, or marriage and or foster children who are so certified by the Texas Health and Human Services Commission and who are living in the same household or, if not in the same household, are totally dependent upon the employee for personal care or services.

Contributing Sick Leave to the Sick Leave Pool

Contributions to the Pool are strictly voluntary and must be in increments of eight hours with the exception of retiring employees, who may contribute any unused balance. However, a retiring employee is advised that donations of 160 hours or more may affect retirement service credit or retirement eligibility.

Employees who make contributions to the Pool may not specify who may use the contributions. Employees are encouraged to contribute to the Pool at the time of their separation from state employment.

An Employee must submit a Sick Leave Pool Transfer form (see Appendix A) through his/her section/division director to be given to the Human Resources Manager designated as the “Pool Administrator.” The amount of sick leave contributed shall be credited to the Pool and shall be deducted from the employee’s accrued sick leave balance.

Use of Sick Leave From the Pool

Employees with catastrophic illnesses or injuries are not required to contribute to the Pool before using leave from the Pool. Employees who use sick leave from the Pool are not required to repay the leave.

Employees absent on assigned sick leave from the Pool shall be treated for all purposes as though absent on earned sick leave.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 9: GENERAL AND MISCELLANEOUS LEAVE

The amount and frequency of the sick leave pool granted for each request will be determined by the Secretary of State and/or the Deputy Secretary of State. The number of hours of leave awarded from the Pool to an employee cannot exceed one-third of the balance of hours in the pool, or 90 workdays, whichever is less. Hours granted to part-time employees shall be on a pro rata basis.

Requests for sick leave from the Pool shall be considered on a first-come, first-served basis.

Any unused balance of sick leave from the Pool granted to an employee shall be returned to the Pool. The estate of a deceased employee is not entitled to payment for unused Pool leave.

Application Procedures

1. To apply to use sick leave pool hours, an employee must submit a memorandum requesting leave from the Pool to the appropriate section/division director for approval. Additionally, the request must include:
 - The Health Care Providers Statement (Appendix A) outlining the injury or illness of the employee or member of immediate family;
 - The treatment required;
 - The requested number of hours;
 - Expected duration of the injury or illness; and
 - The anticipated date of return to work.

2. To have the application approved, the employee must:
 - Have sought approval to use sick leave from the Pool prior to exhausting all accrued leave;
 - Meet the criteria set forth by the Employees Retirement System;
 - Be a full-time or part-time regular employee;
 - Have exhausted all accrued leave;
 - Have shown a consistent effort to make appropriate and conservative use of sick leave benefits;
 - Provide re-certification of catastrophic illness or injury every thirty (30) calendar days; and
 - Intend to return to work with the Agency.

Upon receipt and approval of the request to use sick leave pool, the section/division director shall complete and forward the Application to Use Sick Leave Pool Hours and all documentation to the Human Resources Manager. The Human Resources Manager shall ensure that the request meets Agency policy and shall determine the exact amount of sick leave that an employee may use from the Pool and forward the application to the

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 9: GENERAL AND MISCELLANEOUS LEAVE

Secretary of State or the Deputy Secretary of State, who is the final approving authority. If the Secretary of State or the Deputy Secretary of State approves the application, the leave shall be credited to the employee, who may use the leave for the documented illness or injury.

The Secretary of State or Deputy Secretary of State shall consider each application on its own merits on an individual basis. The Secretary of State or the Deputy Secretary of State may make exceptions to the listed Pool requirements after review of the merits of an individual case.

9.5 EXTENDED SICK LEAVE

An employee who is temporarily unable to work due to illness or injury that necessitates the employee being off work for a period of time that exceeds two (2) work weeks and who has exhausted or will soon exhaust all accrued leave may be granted Extended Sick Leave. Requests for Extended Sick Leave will be based upon exceptional circumstances, will be fully justified, and will require approval by the Secretary of State or the Deputy Secretary of State. The granting of Extended Sick Leave is discretionary and will be approved only upon determination that it is in the best interest of the Agency. Extended Leave is not available for the illness or injury of an employee's immediate family member.

Each request shall be considered on its own merits and, if approved, the total leave granted for each illness or injury will be equal to the employee's cumulative leave balances as of September 1st of the current fiscal year, but will not exceed the following:

- Employees with five (5) years or less of state service – maximum of 176 hours
- Employees with over five (5) years of state service – maximum of 240 hours
- Employees with over twenty (20) years of state service – maximum of 360 hours

Hours granted to part-time employees shall be on a pro rata basis.

Eligibility

To be eligible for extended sick leave, the employee must:

- Be a full-time or part-time regular employee;
- Have been continuously employed in state government for at least one (1) year;
- Be currently performing job duties at a satisfactory level according to the manager/team leader, and as reflected in the employee's performance evaluation on file in the Human Resources Department;
- Have exhausted all accrued leave;
- Use leave from the sick leave pool prior to applying for extended leave, if eligible;
- Have shown a consistent effort to make appropriate and conservative use of sick leave. Sick leave consistently depleted as it is accrued, failure to maintain sick leave

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 9: GENERAL AND MISCELLANEOUS LEAVE

balances without good cause, or a pattern of using sick leave on Mondays, Fridays, or days immediately before or after a holiday may be evidence of unacceptable use of sick leave;

- Provide re-certification of illness or injury every thirty (30) calendar days; and
- Intend to return to work with the Agency.

Application Procedures

To apply for extended sick leave, an employee must submit a memorandum requesting Extended Sick Leave to the appropriate section/division director for approval. Additionally, the request must include:

- The Health Care Providers Statement (See Appendix A) outlining the injury or illness of the employee;
- The treatment required;
- The requested number of hours;
- Expected duration of the injury or illness; and
- The anticipated date of return to work.

Award of Extended Sick Leave

Upon receipt and approval of a request for Extended Sick Leave, the section/division director shall complete and forward the Application to Use Extended Sick Leave and all documentation to the Human Resources Manager. The Human Resources Manager shall ensure that the request for Extended Sick Leave meets Agency policy and shall determine the exact amount of extended sick leave that may be offered to the employee and forward the application to the Secretary of State or the Deputy Secretary of State for final approval. If the Secretary of State or the Deputy Secretary of State approves the application, the leave shall be credited to the employee, who may use the leave for the documented illness or injury.

The estate of a deceased employee is not entitled to payment for unused extended sick leave granted to the employee.

9.6 LEAVE WITHOUT PAY (LWP)

Leave without pay, except under the provisions of the FMLA, is not a right granted to employees, but is a privilege afforded in instances approved by an employee's section/division director.

Provisions

Employees may be granted LWP subject to the following provisions.

1. Except for disciplinary suspensions, active military duty, and workers' compensation situations, all accrued leave (including state compensatory and FLSA compensatory time balances) must be exhausted before such leave may be

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 9: GENERAL AND MISCELLANEOUS LEAVE

- granted, with the additional provision that sick leave must be exhausted only in those cases where the employee is eligible to use sick leave, as provided in Section 9.3 above.
2. Deductions for LWP are calculated on a workday basis.
 3. Employees on LWP for an entire calendar month, with the exception of those on leave in accordance with the FMLA, are responsible for paying 100 percent of the monthly health insurance premium. The HRD and the ERS will notify the employee in writing of the amount due and the due date.
 4. Employees will not receive service credit, longevity pay, annual leave, or sick leave accruals for any full calendar month of LWP. Any full calendar month of LWP shall not constitute a break in employment, but shall not be included in the calculation of the minimum number of continuous months of state service required under merit raise, annual leave, or other leave provisions.
 5. Employees who exhaust their military leave (See **Military Leave** below) are entitled to a leave of absence. Employees may elect to substitute all or some paid leave before going on LWP and shall continue to accrue state service credit for purposes of longevity pay, and accruing annual leave and sick leave and shall receive such credit upon return to state employment.
 6. Such leave shall be limited in duration to twelve (12) months.
 7. The Secretary of State or the Deputy Secretary of State may grant exceptions to these limitations for reasons determined appropriate including interagency agreements or educational purposes.

Notification/Implementation of Leave Without Pay Status

1. All LWP must be reported to the HRD by noon on or before the 15th of each month. Divisions/sections will be notified of exceptions to this policy when payroll deadlines require earlier submission. This notification shall be accomplished by the appropriate section/division director submitting to the HRD a copy of the original timesheet for the employee on LWP indicating all leave taken, including leave without pay, to date. Additionally, section/division directors must notify the HRD promptly, by memorandum or e-mail, when an employee has requested extended leave without pay.
2. Employees must follow established rules and provide proper documentation concerning annual leave and/or sick leave when being placed on LWP because of insufficient accrued leave.
3. Timesheets shall be submitted by noon on the last working day of the month indicating all leave taken for the entire pay period.

9.7 MILITARY LEAVE – See Section 13: Military Leave and Employment Rights

9.8 PARENTAL LEAVE

An employee who is not eligible for leave under the Family Medical Leave Act (FMLA) may be entitled to “Parental Leave” in lieu of leave under the FMLA.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 9: GENERAL AND MISCELLANEOUS LEAVE

“Parental Leave” is defined as a leave of absence which shall not exceed twelve (12) weeks for the birth of a child, adoption of a child or placement of a foster child under three (3) years of age. This leave begins with the date of birth, adoption, or foster care placement. Employees are required to use accrued leave while on Parental Leave and are placed on leave without pay for any remaining period. However, the use of sick leave during the twelve (12) week period or anytime exceeding the twelve (12) weeks is strictly limited to those situations falling within the definition of “sick leave” contained in this section. Time off exceeding the twelve (12) week period may be granted if approved by the section/division director.

9.9 MISCELLANEOUS LEAVE

- **Administrative Leave** - The Secretary State or the Deputy Secretary of State may grant a maximum of thirty-two (32) hours of administrative leave per fiscal year as a reward for outstanding performance as documented by employee performance appraisals.
- **Amateur Radio Operator** – An employee who holds an amateur radio station license issued by the Federal Communications Commission may be granted leave not to exceed ten (10) days each fiscal year to participate in specialized disaster relief services without a deduction in salary or loss of annual or sick leave, accrued overtime, or state compensatory time if the leave is taken with the authorization of the employee’s supervisor, and with the approval of the Governor.
- **Assistance Dog Training** - Employees with a disability as defined by Section 121.002, Texas Human Resources Code, will be granted leave not to exceed ten (10) days in a fiscal year to attend training necessary to provide the employee with an assistance dog to be used by the employee. Leave provided by this subsection is in addition to other leave to which the employee is entitled, and the employee will continue to accrue vacation and sick leave while on leave. To attend a training program, an employee must submit a memorandum to the section/division director for approval. The memorandum must contain the dates of the training.
- **Blood Donation** - Employees shall be allowed sufficient time off, without a deduction in salary or accrued leave, to donate blood. An employee may not receive time off to donate blood unless the employee obtains approval from his/her manager/team leader before taking time off. Upon returning to work, an employee shall provide the employee’s manager/team leader with proof of the donation during the time off. If an employee fails to provide proof, the Agency shall deduct the period for which the employee was granted time off from the employee’s salary or accrued leave, at the employee’s option. An employee may receive time off under this section not more than four (4) times in a fiscal year.
- **Bone Marrow or Organ Donation** - Employees are entitled to leave of absence without a deduction in salary for the time necessary to serve as bone marrow or organ donors. The leave of absence provided by this section may not exceed:
 - Five (5) working days in a fiscal year to serve as a bone marrow donor; or

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 9: GENERAL AND MISCELLANEOUS LEAVE

- Thirty (30) working days in a fiscal year to serve as an organ donor.
- **Certified American Red Cross Activities** - Employees who are certified disaster service volunteers of the American Red Cross (ARC) or who are in training to become such a volunteer may be granted paid leave not to exceed ten (10) days each fiscal year to participate in specialized disaster relief services for the ARC. The employee must obtain approval from his/her supervisor and the Governor and receive a formal request from the ARC.
- **Court Appointed Special Advocates Volunteer** - Employees may be granted leave not to exceed five (5) hours each month to participate in mandatory training or perform volunteer services for Court Appointed Special Advocates without a deduction in salary or loss of annual leave, sick leave, earned overtime credit, or state compensatory time.
- **Emergency Leave** - The death of an employee's spouse or the employee's or spouse's parent, brother, sister, grandparent, grandchildren, or children (including present, but not former, stepchildren) shall constitute adequate need for Emergency Leave. Such leave may be granted by the appropriate section/division director for the time required for funeral preparations, grieving, and to attend the funeral and shall not exceed three (3) non-consecutive working days unless the Secretary of State or the Deputy Secretary of State approve additional time. The Secretary of State or the Deputy Secretary of State may grant emergency leave when he or she determines that the employee shows good cause for such leave. For an employee to be granted emergency leave, the employee must be in a paid status.
- **Foster Parent Leave** - An employee who is a foster parent to a child under the protection of the Texas Department of Family and Protective Services (DFPS) is entitled to paid leave of absence to attend staff meetings held by the DFPS regarding the foster child and to attend admission, review, and dismissal meetings held by a school district regarding the foster child.
- **Compliance with Subpoena** - Employees called to appear in an official capacity in any judicial action or legislative investigation shall neither accept nor receive any witness fees for such governmental appearance. However, if the appearance is not in an official capacity, but is for the purpose of testifying from personal knowledge, then an employee may accept any customary witness fees. In this latter case, the employee must use his/her accrued leave. The limitations relating to witness fees do not extend to any mileage or per diem allowance paid to the employee for expenses incurred while serving as a witness unless the employee has also made a claim for such expenses against the state. In no instance shall there be double reimbursement for expenses.
- **Jury Service** - Employees called for jury service are granted paid leave for time served. Any compensation or reimbursement of expenses received for jury service shall not affect wages paid. Employees must submit and attach with timesheets proof of jury service from the court indicating actual time served. A jury summons is insufficient evidence of jury service.
- **Parent-Teacher Conference** - An employee may use sick leave each fiscal year to attend parent-teacher conference sessions for the employee's children who are in pre-

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 9: GENERAL AND MISCELLANEOUS LEAVE

kindergarten through 12th grade. Full-time employees may use up to eight (8) hours of sick leave. Part-time employees may use a proportionate number of hours of sick leave. Employees must give reasonable notice of intention to use sick leave to attend such conferences.

- **Time Off to Vote** - Employees are entitled to sufficient time off with no deduction in salary to vote in each national, state, or local election on a uniform election day. However, employees are not entitled to time off during early voting.
- **Volunteer Firefighters' Leave/Emergency Medical Services Training** -Employees who are volunteer firefighters or emergency medical services volunteers are entitled to paid leave not to exceed five (5) working days per fiscal year to attend training services conducted by state agencies or institutions of higher education. Additionally, the Agency will grant leave (not to be charged against the employee's annual or sick leave) with full pay to volunteer firemen or emergency medical services volunteer for the purpose of responding to emergency fire or medical situations.

9.10 TRANSFER OF ACCRUED LEAVE

Annual Leave - Employees who transfer or are re-employed within 30 calendar days by another state agency to a position that accrues annual leave are entitled to transfer accrued annual leave.

Sick Leave - Employees who terminate employment under a formal reduction in force are entitled to have their sick leave balances restored if they are re-employed by the State within 12 months.

Employees who terminated for reasons other than a formal reduction in force and who have subsequently been re-employed by the same state agency or institution of higher education may have their sick leave balances restored only if:

- The employee is re-employed by the same state agency or institution of higher education within 12 months after the end of the month in which the employee terminated employment and if there has been a break in employment with the state of at least 30 calendar days; or
- The employee is re-employed by another state agency or institution of higher education within 12 months after the end of the month in which the employee terminated employment.

“State Agency” refers to any state agency or institution included in the Appropriations Bill, regardless of the Article in which it appears. Contact the HRD for aid in establishing prior state service or in transferring annual and sick leave from such prior service.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 9: GENERAL AND MISCELLANEOUS LEAVE

9.11 CREDIT FOR ACCUMULATED ANNUAL LEAVE AND SICK LEAVE

Employees hired on or before August 31, 2009, who retire based on service or disability are entitled to service credit for accrued but unused annual leave and sick leave on the last day of employment. Employees are eligible to receive one (1) month of service credit for each 160 hours, or fraction thereof, of unused sick leave and annual leave. This service credit may be used to satisfy requirements for retirement, insurance eligibility, and to increase annuity benefits.

9.12 ABSENCE FROM WORK BECAUSE OF INCLEMENT WEATHER

If inclement weather is so severe that all or most employees of the Agency would be endangered by hazardous driving conditions either in arriving to work or in returning home from work at the regular time, the Secretary of State or the Deputy Secretary of State shall declare an emergency and shall permit employees to be absent from work without charge against any available leave or loss of pay. Under such circumstances, the Secretary of State or the Deputy Secretary of State shall issue a notice to the division directors who shall take the necessary action to notify all employees. Employees should contact the HRD at 463-8000 for a recorded message regarding agency closures. This absence shall be charged as Emergency Leave-Other (EO) and reported as a permitted absence.

If an employee decides not to report to work because of a determination that hazardous driving conditions prevent the employee from reporting to work or returning home at the regular time, then the employee shall notify a manager/team leader of such decision and shall request leave for that business day. The manager/team leader shall grant the employee's request for leave unless the manager/team leader determines that the employee's services are indispensable. Such absence from work shall be charged against accrued leave. An employee who does not have enough leave to cover the absence shall be placed on LWP for the period of time not covered by the employee's leave. Sick leave shall not be used unless the employee or the employee's immediate family is ill or injured.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 10: HOLIDAYS

10.0 GENERAL

Employees are entitled to a paid day off from work on national, state, and optional holidays observed by the state. However, the Agency will remain open and have enough personnel to conduct business on state holidays.

If a holiday falls in mid-month (other than the first or last workday of the month), employees must be a state employee on the day before and the day after the holiday. If the holiday falls on the first workday of a month, employees must be a state employee on the day immediately after the holiday. If the holiday falls on the last workday of the month, employees must be a state employee on the day immediately before the holiday. For purposes of determining entitlement to a paid holiday, “state employee” is defined as being employed by the state and not on leave without pay.

Employees who work during a national holiday or a state holiday period shall be allowed holiday compensatory time off during the twelve-month period following the date of the holiday worked. Employees who telecommute do not earn holiday compensatory leave if they work on a holiday at home. (Compensatory time is subject to the provisions outlined in Section 6.)

An employee working a non-traditional schedule who works less than the entire fiscal year is entitled to paid holiday time off during the fiscal year equal to eight hours multiplied by the number of national and state holidays that occur during the time period worked by the employee.

NATIONAL HOLIDAYS

- the 1st day of January, “New Year’s Day”
- the 3rd Monday in January, “Martin Luther King, Jr., Day”
- the 3rd Monday in February, “Presidents’ Day”
- the last Monday in May, “Memorial Day”
- the 4th day of July, “Independence Day”
- the 1st Monday in September, “Labor Day”
- the 11th day of November, “Veterans Day”
- the 4th Thursday in November, “Thanksgiving Day”
- the 25th day of December, “Christmas Day”

STATE HOLIDAYS

- the 19th day of January, “Confederate Heroes Day”*
- the 2nd day of March, “Texas Independence Day”*
- the 21st day of April, “San Jacinto Day”*
- the 19th day of June, “Emancipation Day in Texas”*
- the 27th day of August, “Lyndon Baines Johnson Day”*

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 10: HOLIDAYS

- the Friday after Thanksgiving Day
- the 24th day of December
- the 26th day of December

*On these days, the Agency shall have enough personnel to conduct public business. However, this does not apply to a state holiday that falls on a Saturday or Sunday, on the Friday immediately following the fourth Thursday in November, on the 24th day of December, or on the 26th day of December.

Unless authorized by the Secretary of State or Deputy Secretary of State, the Agency will not close on another day when designated holidays fall on Saturday or Sunday.

10.1 OPTIONAL HOLIDAYS (SUBSTITUTE HOLIDAY LEAVE)

Employees are entitled to substitute Rosh Hashanah, Yom Kippur, Cesar Chavez Day, and Good Friday in lieu of any state holiday(s), during the same fiscal year in which the Agency is required to be open and staffed to conduct public business provided that the employee does not agree to give up the Friday after Thanksgiving Day, Christmas Eve, or December 26th. Employees cannot substitute optional holidays for a national holiday.

To request Substitute Holiday Leave (SHL), employees must obtain approval from the appropriate section/division director. Upon approval, an employee must annotate in the Justification column of the timesheet what state holiday the employee will work. For example, an employee that wants to observe Cesar Chavez Day will write “SHL (San Jacinto Day)” in the Justification column of the timesheet on Cesar Chavez Day.

The HRD shall maintain balances indicating hours worked/taken, but it shall be the responsibility of each division/section director to ensure that those employees work and/or take the requested holidays during the fiscal year. At the end of the fiscal year, the HRD shall purge all negative balances and make adjustments to leave balances or pay as required. Under no circumstances shall a negative balance be carried forward into the next fiscal year.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 11: FAMILY AND MEDICAL LEAVE ACT (FMLA)

11.0 INTRODUCTION

The Family Medical Leave Act (FMLA) of 1993 entitles eligible employees to take up to 12 weeks of unpaid, job-protected leave in a 12-month period for specified family and medical reasons. Amendments to the FMLA by the National Defense Authorization Act for FY 2008 (NDAA), Public Law 110-181, expanded the FMLA to allow eligible employees to take up to 12 weeks of job-protected leave in the applicable 12-month period for any “qualifying exigency” arising out of the fact that a covered military member is on active duty, or has been notified of an impending call or order to active duty, in support of a contingency operation. The NDAA also amended the FMLA to allow eligible employees to take up to 26 weeks of job-protected leave in a “single 12-month period” to care for a covered servicemember with a serious injury or illness.

11.1 EMPLOYEE ELIGIBILITY

To be eligible for FMLA benefits, an employee must:

- have worked for the Agency for a total of 12 months; and
- have worked at least 1,250 hours over the previous 12 months.

While the 12 months of employment need not be consecutive, employment periods prior to a break in service of seven years or more need not be counted unless the break is occasioned by the employee’s fulfillment of his or her National Guard or Reserve military obligation (as protected under the Uniformed Services Employment and Reemployment Rights Act (USERRA)).

11.2 LEAVE ENTITLEMENT

The Agency will grant an eligible employee up to a total of 12 workweeks of unpaid leave during any 12-month period for one or more of the following reasons:

- for the birth and care of a newborn child of the employee;
- for placement of a son or daughter for adoption or foster care with the employee;
- to care for a spouse, son, daughter, or parent with a serious health condition;
- to take medical leave when the employee is unable to work because of a serious health condition; or
- for qualifying exigencies arising out of the fact that the employee’s spouse, son, daughter, or parent is on active duty or call to active duty status as a member of the National Guard or Reserves in support of a contingency operation.

The 12 month period is determined by measuring backward from the date an employee uses FMLA leave. An employee is entitled to use up to 12 weeks of job-protected leave during a 12 month period. Under this policy, each time an employee takes FMLA leave the remaining leave entitlement would be any balance of the 12 weeks which has not been used during the immediately preceding 12 months.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 11: FAMILY AND MEDICAL LEAVE ACT (FMLA)

The Agency will also grant an eligible employee who is a spouse, son, daughter, parent, or next of kin of a current member of the Armed Forces, including a member of the National Guard or Reserves, with a serious injury or illness up to a total of 26 workweeks of unpaid leave during a “single 12-month period” to care for the servicemember.

Spouses employed by the same Agency are limited in the amount of family leave they may take for the birth and care of a newborn child, placement of a child for adoption or foster care, or to care for a parent who has a serious health condition to a combined total of 12 weeks (or 26 weeks if leave to care for a covered servicemember with a serious injury or illness is also used). Leave for birth and care, or placement for adoption or foster care, must conclude within 12 months of the birth or placement.

Under some circumstances, employees may take FMLA leave intermittently – taking leave in separate blocks of time for a single qualifying reason – or on a reduced leave schedule – reducing the employee’s usual weekly or daily work schedule. When leave is needed for planned medical treatment, the employee must make a reasonable effort to schedule treatment so as not to unduly disrupt the Agency’s operation. If FMLA leave is for birth and care, or placement for adoption or foster care, use of intermittent leave is subject to the Agency’s approval.

Employees must “substitute” (run concurrently) all accrued paid leave to cover some or all of the FMLA leave.

Note: It is the Agency’s right, not the employee’s right, to designate FMLA-qualifying leave as such. Therefore, any FMLA-qualifying leave taken by an eligible employee shall be so designated and thus counted against the employee’s total FMLA entitlement.

11.3 DEFINITIONS

“Serious health condition” means an illness, injury, impairment, or physical or mental condition that involves either:

- Inpatient care (i.e., an overnight stay) in a hospital, hospice, or residential medical-care facility, including any period of incapacity (i.e., inability to work, attend school, or perform other regular daily activities) or subsequent treatment in connection with such inpatient care; or
- Continuing treatment by a health care provider, including a period of incapacity lasting more than three consecutive, full calendar days and any subsequent treatment or period of incapacity relating to the same condition that also includes:
 - treatment two or more times by or under the supervision of a health care provider (i.e., in-person visits, the first within 7 days and both within 30 days of the first day of incapacity); or
 - one treatment by a health care provider (i.e., an in-person visit within 7 days of the first day of incapacity) with a continuing regimen of treatment (e.g., prescription medication, physical therapy); or

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 11: FAMILY AND MEDICAL LEAVE ACT (FMLA)

- Any period of incapacity related to pregnancy or for prenatal care. A visit to the health care provider is not necessary for each absence; or
- Any period of incapacity or treatment for a chronic serious health condition which continues over an extended period of time, requires periodic visits (at least twice a year) to a health care provider, and may involve occasional episodes of incapacity. A visit to a health care provider is not necessary for each absence; or
- A period of incapacity that is permanent or long-term due to a condition for which treatment may not be effective. Only supervision by a health care provider is required, rather than active treatment; or
- Any absences to receive multiple treatments for restorative surgery or for a condition that would likely result in a period of incapacity of more than three days if not treated.

11.4 MAINTENANCE OF HEALTH BENEFITS

The Agency will maintain group health insurance coverage for an employee on FMLA leave whenever such insurance was provided before the leave was taken and on the same terms as if the employee had continued to work. If applicable, arrangements will need to be made for employees to pay their share of health insurance premiums while on leave. In some instances, the Agency may recover premiums it paid to maintain health coverage for an employee who fails to return to work from FMLA leave.

An employee does not earn state service credit, annual leave, or sick leave for any full calendar months of LWP while on family and medical leave.

11.5 JOB RESTORATION

Upon return from FMLA leave, an employee must be restored to the employee's original job, or to an equivalent job with equivalent pay, benefits, and other terms and conditions of employment. An employee's use of FMLA leave cannot result in the loss of any employment benefit that the employee earned or was entitled to before using FMLA leave, nor be counted against the employee under a "no fault" attendance policy. If a bonus or other payment, however, is based on the achievement of a specified goal such as hours worked or perfect attendance, and the employee has not met the goal due to FMLA leave, payment may be denied unless it is paid to an employee on equivalent leave status for a reason that does not qualify as FMLA leave. An employee has no greater right to restoration or to other benefits and conditions of employment than if the employee had been continuously employed.

An employee returning from FMLA-designated leave taken for his/her own *serious health condition* may be required to provide the Agency with certification (Return To Work Status) from a health care provider that the employee is able to resume work, unless the Human Resources Manager determines that a certification is not required for employees in that situation. For example, the Human Resources Manager may determine

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 11: FAMILY AND MEDICAL LEAVE ACT (FMLA)

that employees returning to work from pregnancy leave need not provide certification that they are no longer pregnant.

11.6 NOTICE

Employee Notice

Employees seeking to use FMLA leave are required to provide a 30-day advance notice of the need to take FMLA leave when the need is foreseeable and such notice is practicable. If leave is foreseeable less than 30 days in advance, the employee must provide notice as soon as practicable – generally, either the same or next business day. When the need for leave is not foreseeable, the employee must provide notice to the employer as soon as practicable under the facts and circumstances of the particular case. Absent unusual circumstances, employees must comply with the Agency’s usual and customary notice and procedural requirements for requesting leave.

Employees must provide sufficient information for the Agency to reasonably determine whether the FMLA may apply to the leave request. Depending on the situation, such information may include that the employee is incapacitated due to pregnancy, has been hospitalized overnight, is unable to perform the functions of the job, and/or that the employee or employee’s qualifying family member is under the continuing care of a health care provider.

When an employee seeks leave for a FMLA-qualifying reason for the first time, the employee need not expressly assert FMLA rights or even mention the FMLA. When an employee seeks leave, however, due to a FMLA-qualifying reason for which the Agency has previously provided the employee FMLA-protected leave, the employee must specifically reference either the qualifying reason for leave or the need for FMLA leave.

Employer Notice

Notices explaining rights and responsibilities under FMLA are posted in the HRD. Additionally, each new employee will receive the aforementioned notice during the New Hire Orientation.

When an employee requests FMLA leave or the Agency acquires knowledge that leave may be for a FMLA purpose, the Agency must notify the employee of his or her eligibility to take leave, and inform the employee of his/her rights and responsibilities under FMLA. When the Agency has enough information to determine that leave is being taken for a FMLA-qualifying reason, the Agency must notify the employee that the leave is designated and will be counted as FMLA leave.

11.7 CERTIFICATION

The Agency may require that an employee’s request for leave due to a serious health condition affecting the employee or a covered family member be supported by a certification from a health care provider. The Agency may require second or third

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 11: FAMILY AND MEDICAL LEAVE ACT (FMLA)

medical opinions (at the Agency’s expense) and periodic recertification of a serious health condition. The Agency may use a health care provider or a member of the HRD staff – but not the employee’s direct supervisor – to authenticate or clarify a medical certification of a serious health condition. If reasonable safety concerns exist, the Agency may, under certain circumstances, require such a certification for employees returning from intermittent FMLA leave.

11.8 MILITARY FAMILY LEAVE ENTITLEMENTS

Military Caregiver Leave:

The Agency will grant up to a total of 26 workweeks of unpaid leave during a “single 12-month period” to an eligible employee who is a spouse, son, daughter, parent, or next of kin of a covered servicemember with a serious injury or illness to care for the servicemember. A covered servicemember is a current member of the Armed Forces, including a member of the National Guard or Reserves, who is undergoing medical treatment, recuperation, or therapy, is otherwise in outpatient status, or is otherwise on the temporary disability retired list, for a serious injury or illness. A serious injury or illness is one that was incurred by a servicemember in the line of duty on active duty that may render the servicemember medically unfit to perform the duties of his or her office, grade, rank, or rating. A covered servicemember is also a veteran who is undergoing medical treatment, recuperation, or therapy for serious injury or illness that occurred any time during the five years preceding the date of treatment. The “single 12-month period” for leave to care for a covered servicemember with a serious injury or illness begins on the first day the employee takes leave for this reason and ends 12 months later, regardless of the 12 month period established by the Agency for other types of leave under the FMLA. An eligible employee is limited to a combined total of 26 workweeks of leave for any FMLA-qualifying reason during the “single 12-month period.” (Only 12 of the 26 weeks total may be for a FMLA-qualifying reason other than to care for covered servicemember.)

Qualifying Exigency Leave:

The Agency will grant an eligible employee up to a total of 12 workweeks of unpaid leave during the normal 12-month period established by the Agency for FMLA leave for qualifying exigencies arising out of the fact that the employee’s spouse, son, daughter, or parent is on active duty, or has been notified of an impending call or order to active duty, in support of a contingency operation. Under the terms of the statute, qualifying exigency leave is available to a family member of a military member on active duty or in the National Guard or Reserves.

Qualifying Exigencies Include:

- Issues arising from a covered military member’s short notice deployment (i.e., deployment on seven or less days of notice) for a period of seven days from the date of notification;

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 11: FAMILY AND MEDICAL LEAVE ACT (FMLA)

- Military events and related activities, such as official ceremonies, programs, or events sponsored by the military or family support or assistance programs and informational briefings sponsored or promoted by the military, military service organizations, or the American Red Cross that are related to the active duty or call to active duty status of a covered military member;
- Certain childcare and related activities arising from the active duty or call to active duty status of a covered military member, such as arranging for alternative childcare, providing childcare on a non-routine, urgent, immediate need basis, enrolling or transferring a child in a new school or day care facility, and attending certain meetings at a school or a day care facility if they are necessary due to circumstances arising from the active duty or call to active duty of the covered military member;
- Making or updating financial and legal arrangements to address a covered military member's absence;
- Attending counseling provided by someone other than a health care provider for oneself, the covered military member, or the child of the covered military member, the need for which arises from the active duty or call to active duty status of the covered military member;
- Taking up to five days of leave to spend time with a covered military member who is on short-term temporary, rest and recuperation leave during deployment;
- Attending to certain post-deployment activities, including attending arrival ceremonies, reintegration briefings and events, and other official ceremonies or programs sponsored by the military for a period of 90 days following the termination of the covered military member's active duty status, and addressing issues arising from the death of a covered military member;
- Any other event that the employee and employer agree is a qualifying exigency.

FMLA leave may be taken intermittently whenever medically necessary to care for a covered servicemember with a serious injury or illness. FMLA leave also may be taken intermittently for a qualifying exigency arising out of the active duty status or call to active duty of a covered military member. When leave is needed for planned medical treatment, the employee must make a reasonable effort to schedule treatment as not to unduly disrupt the Agency's operation.

Certification Requirements:

An employee's request for military family leave must be supported by an appropriate certification. The Agency may require that:

- leave for a qualifying exigency be supported by a copy of the covered military member's active duty orders and certification providing the appropriate facts related to the particular qualifying exigency for which leave is sought, including contact information if the leave involves meeting with a third party; or
- leave to care for a covered servicemember with a serious injury or illness be supported by a certification completed by an authorized health care provider or by a copy of an Invitational Travel Order (ITO) or Invitational Travel Authorization (ITA) issued to any member of the covered service member's family.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 11: FAMILY AND MEDICAL LEAVE ACT (FMLA)

The Agency may authenticate or clarify a medical certification of a serious injury or illness, or an ITO or ITA. Additionally, the Agency may contact the individual or entity named in a certification of leave for a qualifying exigency for purposes of verifying the existence and nature of the meeting.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 12: EMPLOYEE BENEFITS

12.0 GENERAL

The Employees Retirement System of Texas (ERS) administers retirement, health, and other insurance benefits; TexFlex, a tax-savings flexible benefit program; and 401(k) and 457 investment accounts as part of the TexaSaver Program. They also manage and invest the ERS Trust for the sole benefit of retirement system members. Detailed information about these benefits is available from ERS's website at www.ers.state.tx.us.

12.1 INSURANCE

State Contributions of Health Insurance: The State of Texas contributes a percentage of health coverage premiums for employees' and their dependents' health coverage. Full-time employees receive 100 percent of the medical insurance and basic life premiums and 50 percent for dependent medical insurance premiums. Part-time employees receive 50 percent of the medical insurance and basic life premiums and 25 percent for dependent medical insurance premiums.

Health Coverage Waiting Period: New employees without coverage under the Group Benefits Plan (GBP) are subject to a health coverage waiting period of 90 days. The Health Coverage Date is the first of the month following the expiration of the health coverage waiting period.

Premium Conversion: This program is a tax-saving benefit that allows most **GBP** premiums to be automatically deducted from the **employee's** paycheck **before taxes**, including:

- Health and basic term life,
- Dental,
- Optional term life, and
- Voluntary Accidental Death and Dismemberment (AD&D).

No federal income tax or social security tax is assessed on these premiums. The only GBP premiums deducted **after** taxes are:

- Dependent Term Life,
- Short-term Disability insurance, and
- Long-term Disability insurance.

Flexible Spending Account: TexFlex is a tax-savings program authorized by section 125 of the Internal Revenue Code. This program allows employees to set up an account to pay for daycare and healthcare costs with pre-tax money. Employees **do not** pay federal income tax or social security tax on the money that is set aside in a TexFlex account. This type of account is called a Flexible Spending Account (FSA).

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 12: EMPLOYEE BENEFITS

- FSA-Day Care: For eligible day care expenses, and
- FSA-Health: For eligible medical, dental, and other out-of-pocket expenses.

12.2 RETIREMENT AND DEATH BENEFITS

Retirement Benefits

By state statute, employees participate in a defined benefit retirement program authorized by the Texas Legislature. Beginning on the first of the month after the 90th day of employment, 6.5 percent of salary will be deducted and deposited into a personal state retirement account. The state also contributes 6.95 percent to the retirement fund (not into the employee's personal retirement account). Contributions are invested to provide a level of retirement income based on a formula authorized by the Texas Legislature. The ERS website provides detailed information about your ERS retirement benefits, including retirement options, annuity calculation, and insurance eligibility. An estimator on the ERS website will help you calculate an estimate of your retirement annuity.

An employee who first began working for the state on or after September 1, 2009, and former state employees who received a refund of retirement contributions and returned to state employment on or after September 1, 2009, are subject to new retirement benefits changes:⁴

- An employee becomes “vested” and can receive a retirement benefit at age 65 if the employee works for the state for a minimum of 10 years and does not withdraw retirement contributions. Also an employee is vested with 10 years of service when the employee meets the Rule of 80 - when age and service add up to 80. (In both cases, an employee can use five years of military service toward the 10 years.) As a vested employee, an employee may qualify for insurance benefits at retirement.
- An employee may apply unused sick/annual leave to service credit to increase the employee's annuity, but the employee may not use it to attain retirement eligibility.
- If an employee meets the Rule of 80 and retires before age 60, the employee's annuity will be reduced by 5 percent for each year the employee retires before age 60. However, this reduction will be capped at 25 percent.
- Benefits are based on the highest 48 months of salary.

Purchasing Service Credit: An employee can add to service credit by purchasing withdrawn ERS service, waiting period service, and up to 60 months of active duty military service. Additionally, an employee can purchase up to three years of Additional Service Credit (ASC) if the employee is an active employee and has at least 10 years of actual ERS service credit (not counting military service).

TexaSaver: Employees may participate in the TexaSaver Program, a voluntary retirement savings program offered through ERS.

⁴ HB 2559, 81st Legislature

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 12: EMPLOYEE BENEFITS

- **401(k) Plan:** Allows an employee to defer from 1 percent to 99 percent of 401(k) eligible compensation or the yearly maximum, whichever is less. Deferrals must not exceed the yearly maximum set by the IRS. This plan allows an employee to borrow against these funds as well as roll them over to another investment vehicle such as an individual retirement account. See the TexaSaver section of the ERS website.

A new employee with a break in service is automatically enrolled in the 401(k) plan with an opt-out option. One percent of pay is deferred into a Target Date Fund⁵ or other fund(s) as directed by the employee.

- **Roth 401(k) Plan:** Allows employees to make post-tax contributions up to the maximum set by the IRS.
- **457(k) Plan:** Allows an employee to defer a pre-taxed specific dollar amount (\$20 minimum) of salary toward retirement savings. The employee decides how to invest contributions among choices offered by the plan. Deferrals must not exceed the yearly maximum set by the IRS. See the TexaSaver section of the ERS website.
- **Roth 457(k) Plan:** Allows employees to make post-tax contributions up to the maximum set by the IRS.

Death Benefits

The estate of a deceased employee shall receive the following benefits based on the employee's salary rate at the time of death:

- Pay computed through the date of death (less federal withholding and social security taxes);
- Pay for accrued annual leave, provided that the employee had completed at least six (6) months continuous state service;
- Pay for one-half of the employee's accrued sick leave or 336 hour of sick leave, whichever is less, if the employee had at least six (6) months continuous state service;
- Pay for any accrued overtime, if the employee was subject to the overtime provisions of the Fair Labor Standards Act (FLSA); and
- Applicable death benefits under the Employees Retirement System. (These are payable according to the rules and regulations of the ERS and are not always paid to the decedent's estate.)

⁵ HB 957, 80th Legislature

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 13: MILITARY LEAVE AND EMPLOYMENT RIGHTS

13.0 UNIFORMED SERVICES EMPLOYMENT AND REEMPLOYMENT RIGHTS ACT (USERRA)

The U.S. Department of Labor (DOL) Veteran's Employment and Training Service (VETS) administers The Uniform Services Employment and Reemployment Rights Act (USERRA) and all questions should be directed to that office. Contact and additional information about USERRA can be found at www.dol.gov/vets

USERRA prohibits discrimination against persons because of their service in the Armed Forces Reserve, the National Guard, or other uniformed services. USERRA prohibits the Agency from denying any benefit of employment on the basis of an individual's membership, application for membership, performance of service, application for service, or obligation for service in the uniformed services.

The Act protects the right of veterans, reservists, National Guard members, and certain other members of the uniformed services to reclaim their civilian employment after being absent due to military service or training.

Eligible employees may be absent from work for military duty and retain re-employment rights for a cumulative period of five years. Exceptions to the five-year limit include initial enlistments lasting more than five years, periodic National Guard and Reserve training duty, and involuntary active duty extensions and recalls, especially during a time of national emergency. Re-employment protection does not depend on the timing, frequency, duration, or nature of an employee's service as long as the basic eligibility criteria are met.

The USERRA provides protection for disabled veterans, requiring the Agency to make reasonable efforts to accommodate the disability. Employees recovering from injuries received during service or training may have up to two years from the date of completion of service to return to their jobs or apply for re-employment.

Health and Retirement Plan Coverage

Under USERRA, employees performing military duty of more than 30 days may elect to continue employer-sponsored health care for up to 24 months; however, they may be required to pay up to 102 percent of the full premium. For military service of less than 31 days, health care coverage is provided as if the service member had remained employed. USERRA also provides specific protection related to eligibility and participation in pension plans.

Returning Employees

Returning employees are re-employed in the job that they would have attained had they not been absent for military service under USERRA, with the same seniority, status, and pay, as well as other rights and benefits determined by seniority. The Agency is required to make reasonable efforts (such as training or retraining) to enable returning employees

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 13: MILITARY LEAVE AND EMPLOYMENT RIGHTS

to refresh or upgrade their skills to help them qualify for re-employment. The law also provides for alternative re-employment positions if the employee cannot qualify for some positions.

The period in which an employee has to apply for re-employment or report back to work after military service is based on the time spent on military duty. For military service of less than 31 days, the employee must return at the beginning of the next regularly scheduled work period on the first full day after release from service, taking into account safe travel home plus an eight-hour rest period. For military service of more than 30 days but less than 181 days, the employee must submit an application for re-employment within 14 days of release from service. For military service of more than 180 days, an application for re-employment must be submitted within 90 days of release from service. Reporting and application deadlines are extended for up to two years for employees who are hospitalized or convalescing.

Additionally, USERRA requires that employees provide advance written or verbal notice to the Agency for all military duty unless giving notice is impossible, unreasonable, or precluded by military necessity. An employee should provide notice as far in advance as is reasonable under the circumstances. While performing military duty, the employee may use accrued annual leave.

13.1 STATE RE-EMPLOYMENT FOLLOWING MILITARY SERVICE

State law provides that an employee who separates from state service to enlist in the U.S. Armed Forces, Texas State Guard, Texas National Guard, or federal military reserves is entitled to restoration of employment.⁶

The employee is entitled to be re-employed in the same position held at the time when the employee began military service or in a position of similar seniority, status, and pay.

To be eligible for re-employment at the conclusion of military service, the employee must be honorably discharged no later than five years after induction, enlistment, or call to duty and must be physically and mentally qualified to perform the duties of the job.

Applications for Re-employment

Eligible veterans must apply for reinstatement within 90 days after discharge or release from service. The application must be made to the agency or institution of higher education head and must include evidence of discharge.

Re-employment to another Position Following Military Service

If a veteran is unable to perform the duties of the previous job due to a service-related disability, the veteran is entitled to be restored to a position that he or she can perform with similar (same or nearest) seniority, status, and pay. Veterans whose employment

⁶ Texas Government Code, Chapter 613, Reemployment Following Military Service

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 13: MILITARY LEAVE AND EMPLOYMENT RIGHTS

has been restored may not be dismissed without cause within a year of their reinstatement.

Entitlement to Retirement or Other Benefits

An employee re-employed is considered to have been on furlough or leave of absence during the time that the individual was in military service. As such, the employee may participate in retirement or other benefits to which the employee is or may be entitled.

Military Pay Differentials

The Secretary of State or Deputy Secretary of State shall grant emergency leave to provide a pay differential if an employee's military pay is less than the employee's state gross pay. The combination of military pay and emergency leave may not exceed the employee's actual state gross pay. Pay received while assigned to a combat zone, hardship duty pay, and family separation pay is excluded when computing military differential pay.

The Agency will inform activated state employees of the Agency's intent to use emergency leave to supplement their military pay to raise it to a rate comparable to the state pay received prior to activation.

Only employees called to active duty in support of a national emergency or Homeland Security mission (under U.S. Code, Title 10 or Title 32) and whose military pay is less than their gross state pay are eligible for differential pay. Employees involved in routine military training or who are attending military schools are not entitled to this differential pay.

If emergency leave is granted to an employee activated for military duty, the employee will accrue sick leave and annual leave each month they receive pay from the Agency. The sick and annual hours will be accrued but not posted until the employee returns to full employment with the Agency.

Determining Eligibility

To determine eligibility, the employee should provide the Agency a copy of the employee's Military Leave and Earnings Statements (LES) each month that emergency leave is going to be granted to show the total entitlement of military pay received by the employee. The employee's pay may change during the period of active duty because of a promotion or change in entitlements, an increase in pay, or the reduction or ceasing of the need for state military differential pay.

13.2 MILITARY LEAVE ENTITLEMENTS AND ELIGIBILITY

An employee who is called to active duty or authorized military training is entitled to a Leave of Absence (LOA) of fifteen (15) workdays in each federal fiscal year (October 1st

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 13: MILITARY LEAVE AND EMPLOYMENT RIGHTS

through September 30th) without loss of pay or benefits. Employees are eligible for military leave to accommodate:

- Authorized training or duty for the state's military forces, a reserve branch of the U.S. Armed Forces, or state or federally authorized urban search and rescue team.
- National emergency activation for members of a reserve branch of the U.S. Armed Forces.

For leaves of absence beyond fifteen (15) workdays, please see Section 9, General and Miscellaneous Leave.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

**SECTION 14: TRAINING, PROFESSIONAL DEVELOPMENT, AND OTHER
BENEFITS**

14.0 ACQUIRED IMMUNE DEFICIENCY SYNDROME (AIDS) AND HUMAN IMMUNODEFICIENCY VIRUS (HIV) AWARENESS EDUCATION

During the New Hire Orientation, new employees shall receive a copy of the Agency's workplace guidelines and an educational pamphlet published by the Texas Department of State Health Services.

All employees shall receive annual training and education about HIV/AIDS and its implications in the workplace. This shall include the current medical information about HIV/AIDS transmission and methods of prevention, confidentiality and related laws, and nondiscrimination.

14.1 EQUAL EMPLOYMENT OPPORTUNITY (EEO) STANDARDS

Employees shall receive employment discrimination training, including employment discrimination involving sexual harassment. New employees must receive employment discrimination training no later than 30 days after the date of hire. Employees who complete the training are required to sign a statement, which shall be placed in each employee's personnel file, verifying his/her completion of the training program.

Additional employment discrimination and sexual harassment training is required for each employee every two years after employment.

14.2 PROFESSIONAL DEVELOPMENT AND TRAINING

The Agency encourages employees to enhance their knowledge, skills, and abilities through educational and training programs.

Career Development Programs - Employee are encouraged to use workshops, seminars, institutes, training sessions, on-the-job training, and other one-time programs to help improve professional or technical knowledge in current or prospective duty assignments, and to provide training for particular tasks. This includes advanced computer related technical training; although employees receiving advanced computer training are subject to the obligations listed below. With an approved Purchase Requisition, registration fees for such programs are billed directly to the Agency.

14.3 OBLIGATIONS ASSUMED BY PARTICIPATING EMPLOYEES

Employees can find a Training Matrix in Appendix C. This matrix includes new employee training and training that is required every two years for all employees.

Team Leaders have access to MindLeaders which is an e-learning system. The courses that are available range from technical, customer service, management, and Microsoft

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

**SECTION 14: TRAINING, PROFESSIONAL DEVELOPMENT, AND OTHER
BENEFITS**

learning packages. All Team Leaders are required to complete four MindLeader courses each fiscal year.

Professional Licenses - The Agency shall support the efforts of employees holding job-related professional licenses to meet the continuing professional education requirements to maintain their licenses.

Continuing Higher Education Program - The State Employees Training Act authorizes the Agency to use public funds to provide training and education to employees at an institution of higher education for current or prospective job duties. The Agency shall consider reimbursement of required costs for such continuing education to qualified employees when funds are available in the division budget.

An “institution of higher education” is any public technical institute, public junior college, public senior college or university, medical or dental unit, public state college, or other agency of higher education as defined by Section 61.003, Education Code.

“Required costs” are those costs that every student must pay to be enrolled in the institution or in the course(s) for which the employee registers, including tuition, required fees and books. Employees shall be responsible for such items as parking fees, refundable property fees, deposits, and late fees.

Eligibility

Employees must:

- Be a regular, full-time employee;
- Have At least twelve (12) continuous months of employment with the Agency before applying for financial assistance; and
- Not be subject to any Agency disciplinary action at the time reimbursement is requested.

Application Procedures

Employees must submit the following documents:

- Application for Financial Assistance (Application) before beginning or incurring any costs (see Appendix A – Forms). The Application shall identify the course(s) to be taken, costs of tuition, fees and books, and shall also specify leave accounting procedures to be followed by the employee. The section/division director and the Secretary of State/Deputy Secretary of State must approve the Application.
- Continuing Education Program Memorandum of Agreement (Agreement) which, together with all exhibits and attachments thereto, shall constitute the Agreement

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

**SECTION 14: TRAINING, PROFESSIONAL DEVELOPMENT, AND OTHER
BENEFITS**

between the employee and the Agency (see Appendix A – Forms). The employee must sign and obtain approval from the section/division director. For the second and any succeeding semesters for which the employee applies to participate in this program, only the Application needs to be completed and attached to the original Agreement.

The Agreement is subject to termination by the Secretary of State, Deputy Secretary of State, or division director at any time by written notice to the employee and the section director, should it be determined that fulfilling the Agreement would be unreasonable or unduly burdensome. The Agreement is not required if the total course cost does not exceed \$300.00. The Agreement is to be executed in triplicate. The original will be filed in the employee's Personnel File and the employee and section/division director will retain a copy.

Required Documentaion:

- Copy of most recent performance evaluation.
- A memorandum describing how each course is either directly work related or will enhance his/her knowledge/performance in his/her current or prospective job.
- Proof of completion of required academic prerequisites if requested by the section/division director.
- Memorandum justifying attendance to a private educational institution, if applicable.
- Purchase Requisition. This will encumber the funds if the training is provided.

Course Requirements

- Courses do not have to be directed toward a specific degree but must be either directly work related or must serve to enhance the employee's knowledge and/or performance in his/her current or prospective job duties.
- Courses taken at a college or university must be taken for grade credit; an exception to the grade credit requirement may be granted for certain work-related technology courses. Fees for audited courses cannot be reimbursed. Fees for courses taken on a pass/fail or credit/no credit basis cannot be reimbursed unless the educational institution does not offer the course on a grade basis.
- A grade of "C," "70," or "2.0," or better must be attained for each course. When a course is not offered for a grade, "Pass" or "Credit" is required for reimbursement to be considered. The employee must submit, along with the request for reimbursement, an official grade report.
- Generally, employees must take continuing higher education courses using accrued leave or while outside of normal business hours. However, if the course requires a schedule other than 8:00 a.m. to 5:00 p.m., the employee must request a flextime schedule approved by the section/division director, in accordance with the Agency's flextime policy. The section/division director, upon approval by the Secretary of

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

**SECTION 14: TRAINING, PROFESSIONAL DEVELOPMENT, AND OTHER
BENEFITS**

State or the Deputy Secretary of State, may designate a directly job-related course as part of the employee's regular duty assignment, for which no leave would be charged.

- Employees must take lower division courses that are offered by a public institution that satisfy the degree requirements of a private institution.
- Employees who pursue a course of study must provide a degree plan from the course catalogue or from an academic advisor verifying that the courses are required for the degree plan.
- Special Rules for Non-traditional Credit Hours - College Level Equivalency Program (CLEP) exams, correspondence courses from an accredited college or university, and life experience assessments must apply toward an approved degree plan or must be approved as being job related.

Reimbursement Policy

Required costs shall be reimbursed for up to six (6) credit hours each semester. For employees enrolled in an ongoing course of study or certification program, reimbursement may be determined on a course by course basis.

Reimbursement shall not exceed the cost for hours taken at a public university or community college in Austin. Reimbursement for required costs at a private institution will be considered only if the courses are part of a degree plan and:

- No public institution within commuting distance offers similar courses; or
- The employee can demonstrate satisfactorily that completion of the degree at a private institution will be less costly overall, in terms of money and/or time required, to the Agency than completion of the same degree at a public institution.

Costs that can be reimbursed for non-traditional credit hours are limited as follows:

- CLEP – Reimbursement cannot exceed the actual cost of the exam.
- Correspondence course – Reimbursement shall be considered for the actual course fee, but shall not exceed the cost for the same number of credit hours at a public institution.
- Life Experience Assessment – Reimbursement cannot exceed the cost for the same number of credit hours at a public institution, unless the employee can demonstrate satisfactorily that completion of a degree plan using the non-traditional credit hours would be less costly overall, in terms of money and/or time required, to the Agency than completion of the same degree using traditional credit hours.

Note: Reimbursement for non-traditional credit hours is also subject to the credit hour limitation described above.

- Termination of employment for whatever reason releases the Agency from the obligation of reimbursement under the Continuing Higher Education Program.
- The section/division director will submit the employee's receipts for tuition and compulsory fees, official grade report, and a memorandum requesting payment of the

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

**SECTION 14: TRAINING, PROFESSIONAL DEVELOPMENT, AND OTHER
BENEFITS**

encumbered requisition if all criteria has been met for consideration of reimbursement.

Obligations Assumed by Participating Employees

Employees who receive financial assistance for continuing education from the Agency will be obligated to fulfill the terms and conditions below. This obligation also applies to employees who receive advanced computer-related technical training at an annual cost of \$5,000 or more.

- The employee is bound by all terms and conditions of the Agency's Continuing Higher Education Program described herein and by such other applicable policies and procedures as may be promulgated by the Secretary of State.
- The employee must remain in the employ of the Agency for a fixed period of time (see below) subsequent to the completion of any higher education coursework or advanced computer-related technical training under this program.
- The obligation period shall be one (1) month for each \$500 of reimbursement, but shall not exceed twelve (12) months following the completion of training. If the employee is enrolled in a continuing course of study or certification program or advanced computer-related technical training, the obligation to remain employed begins upon completion of the entire program rather than the completion of each individual course within such program.
- If the employee resigns from the Agency before completing the degree program, certification program, coursework, or advanced computer-related technical training, or becomes in default of any of the provisions of the Continuing Higher Education Program, he/she must agree to repay in a lump sum, or by such alternate arrangements as the Secretary of State or Deputy Secretary of State may prescribe, the amount of money expended by the Agency for his/her required education costs provided. If a default is based on the employee's failure to fulfill the continued employment obligation period, the total liability of the employment shall be reduced pro rata based on the length of actual employment credited toward the fulfillment of such period. Calculations for repayment amounts will be rounded to whole months. However, the employee is not obligated to repay, as outlined above, should he/she be involuntarily terminated due to budgetary cutbacks, reduction in force, Agency reorganizations, or disciplinary action.

14.3 PARKING

Parking - The employee parking area is under the jurisdiction of the Texas Department of Public Safety Monday through Friday from 7:30 a.m. to 6:00 p.m. and under the administration of the Agency. Employees must contact the Agency's Parking Coordinator to obtain a parking decal. Three (3) types of parking are available to employees of the Agency.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

**SECTION 14: TRAINING, PROFESSIONAL DEVELOPMENT, AND OTHER
BENEFITS**

Open Parking – Employees may park in any garage/lot designated for state employee parking. The following garages and lots are within a five-block radius and are available to agency employees.

- Lot 27 – located at the corner of Congress Avenue and 11th Street. This lot has limited open parking available and parking is on a first come first serve basis.
- Garage A – located on San Jacinto Boulevard at 14th Street and Trinity Street and 14th Street.
- Garage F – located on San Jacinto Boulevard at 13th Street and Trinity Street and 14th Street.
- Garage K – Located at the corner of Brazos Street between 10th Street and 11th Street under the T.J. Rusk Building. This garage has limited parking spaces that are assigned on a proportionate basis by division/section and each employee’s current employment date. Current employment date is defined as the most recent hire date for an employee at this Agency. All employees are on a waiting list for Garage K. When an employee resigns, HR will then notify the next employee in that section of their parking assignment to Garage K.

Reserved Parking – There are a limited number of Agency reserved parking spaces. At the discretion of the Secretary of State/Deputy Secretary of State, these spaces will be assigned to key management personnel.

Disabled Parking – Parking spaces specifically designated for disabled employees are located in employee parking lots near the Capitol Complex and state buildings.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 15: GRIEVANCE POLICY

15.0 RIGHT TO PRESENT GRIEVANCE

Section 617.005 of the Texas Government Code preserves the rights of state employees to present grievances concerning their wages, hours, or conditions of work. “Conditions of work” is to be construed broadly to include any matter that is appropriate for communications between employees and employer concerning an aspect of their relationship, including but not limited to disciplinary actions or terminations. In order to present a grievance, an employee must follow the procedures set forth below.

15.1 REPRESENTATION

Employees may present the grievance personally or through a designated representative.

15.2 EXPENDITURES FOR REPRESENTATIVES OF GRIEVANTS PROHIBITED

No state funds may be used to pay expenses for salary, travel, or per diem of public employees who represent grievants in the presentation of grievances, except that state employees are allowed to use annual leave, compensatory leave, or leave without pay, subject to the procedures established by the Agency, to engage in this activity.

15.3 GENERAL PROVISIONS

- An employee has the right to present a grievance. The grievance procedure ensures that employees have access to those in position of authority to present their grievances. The Secretary of State and the representatives of the Secretary of State are not required to take action on a grievance other than those specified in the procedures below.
- Grievances should generally first be presented to the employee’s manager. If the grievance is against the employee’s team leader, the employee should present the grievance to the section director. If the grievance is against the employee’s section director, the employee should present the grievance to the division director. If the grievance is against the employee’s division director, the employee should present the grievance to the Deputy Secretary of State.
- The Human Resources Manager shall review all responses to grievances prior to issuance to ensure consistency of application.
- The grievance shall be considered resolved if action to notify the Agency of the existence of a grievance or action to initiate an appeal of a decision is not taken by the employee within the prescribed time frame, unless the Agency waives the time frame in writing for good cause.

15.4 PROCEDURES

1. Discussion with the Human Resources Manager

An employee may request guidance from the Human Resources Manager as to the process or procedure to follow when filing a grievance. The Human Resources

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 15: GRIEVANCE POLICY

Manager will review the policy and procedures with the employee but will not address the content of the employee's grievance unless the employee is under the supervision of the Human Resources Manager. The Human Resources Manager shall not serve as the employee's advocate in presenting a grievance.

2. Discussion with Manager

Any employee who wishes to present a grievance should file a First Written Grievance with the employee's manager within ten (10) business days of the alleged act or omission that is the subject of the grievance. The manager with assistance from the team leader shall review and investigate the stated grievance. Investigation of the grievance may include interviewing other employees and the review of any and all documentation that would substantiate or invalidate the grievance. The employee will be notified in writing within ten (10) business days of the action, if any, to be taken to address the grievance.

3. Presentation to Section Director

If the grievance is not resolved to the employee's satisfaction, then within five (5) business days after notification of action by the manager and team leader or within twenty-five (25) business days of employee's original grievance (if the manager and team leader fail to respond), the employee shall file a Second Written Grievance with the section director. A copy of the Second Written Grievance shall be forwarded by the employee to the Human Resources Department and shall be included in the employee's personnel file.

The Second Written Grievance shall set forth:

- the complaint that is the subject of the grievance;
- the actions, if any, taken by the manager and team leader to address the grievance; and
- the action that the employee requests be taken by the section director to address the grievance.

The section director should schedule an interview with the employee to discuss the grievance. The section director may allow the manager and team leader and other employees having knowledge of the alleged acts of omissions to be present during some or all of the discussion. The section director may interview the manager/team leader or other employees having knowledge of the alleged acts or omissions and may also review all documentation in reference to the grievance.

The section director shall review the Second Written Grievance and within ten (10) business days of the interview notify the employee in writing of the action, if any, to be taken to address the grievance. The notification shall include the reasons for taking or failing to take the requested action. A copy of the notification shall be included in the employee's personnel file, and shall be sent to the employee's manager and team leader.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 15: GRIEVANCE POLICY

4. Presentation to Division Director

If the grievance is not addressed to the employee's satisfaction, the employee may appeal the decision in writing to the division director. The appeal must be made within five (5) business days after the section director's written notification of the action, if any, to be taken to address the Second Written Grievance.

The appeal shall include:

- A copy of the Second Written Grievance submitted to the section director;
- A copy of the Second Written Grievance action, if any, taken by the section director and the reasons for taking or failing to take the action requested; and
- A request for an interview, if desired, regarding the Second Written Grievance.

The division director shall consider the Second Written Grievance and appeal. If the division director determines that additional discussions are necessary to decide what action should be taken, the division director may schedule interviews with the employee, the section director, the manager and team leader, and other employees who may have knowledge relating to the grievance.

Within ten (10) business days after the receipt of the appeal, the division director shall notify the employee in writing of the action, if any, to be taken. A copy of such notification shall be included in the employee's personnel file and sent to the section director and manager and team leader. Such notification shall include the reasons for taking or failing to take action.

5. Final Decision

If the grievance is not addressed to the employee's satisfaction, then within five (5) business days after the notification of the action by the division director, if any, to be taken to address the Second Written Grievance and appeal, the employee shall appeal the decision to the Deputy Secretary of State.

The presentation to the Deputy Secretary of State shall be in writing and include:

- A copy of the Second Written Grievance and the appeal submitted to the section director and the division director; and
- A copy of any actions taken by the director of the section/division.

The Deputy Secretary of State shall review the Second Written Grievance and appeal and the actions, if any, taken to address the grievance and then render a final written decision on the matter. A copy of the written decision shall be included in the employee's personnel file, and be sent to the employee, the division director, the section director, and the manager/team leader.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 15: GRIEVANCE POLICY

15.5 INVOLUNTARY TERMINATION GRIEVANCE

If the Secretary of State or Deputy Secretary of State initiates a termination of employment (i.e., the request for termination is not requested by other persons within the Agency), the employee may file a written grievance directly to the Secretary of State after a waiting period of five (5) business days from the date of termination. All other divisions would follow the standard grievance process stated above.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 16: OFFICE MANAGEMENT

16.0 GENERAL COMMENTS

Employees have a responsibility to the Agency and to the people of Texas to further the efficient operation of the Agency. Employees are expected to properly perform the functions of their jobs and to observe the guidelines for operation of the Agency and the buildings it occupies. These rules and regulations, promulgated by the Secretary of State, are designed to assist employees in achieving their goals and discharging their duties.

16.1 DOCUMENT RETENTION

The Human Resources Department (HRD) is responsible for overseeing recordkeeping for all personnel information. Document retention will be in accordance with the Records Retention Schedule. Employees may review their own personnel records and request that a member of the HRD staff make copies of documents in the file.

16.2 OFFICE HOURS

Regular office hours are from 8:00 a.m. to 5:00 p.m., Monday through Friday. Employees may be required to sign in upon arrival and sign out upon leaving. There should be no instance during office hours when a telephone in the Agency is allowed to ring unanswered. During the lunch hour someone should be designated to answer the phone and respond to any questions that may arise. Employees who will not be at their telephones should ensure that their calls are answered by another employee in the office or by a voice mail system.

Employee Breaks and Meal Periods - Full-time employees are entitled to one hour for lunch. Employees may take one 15-minute break in both the morning and afternoon as the employee's work schedule permits. If an employee does not take a break, the employee's break does not accumulate for future usage. Breaks are not required by federal law or state statute.

16.3 FLEX TIME (STAGGERED WORK HOURS)

All Agency functions shall be fully covered during regular office hours. "Flexitime," or work hours beginning as early as 7:00 a.m. and ending as late as 6:00 p.m., must be approved by the section/division director in individual instances based upon the following guidelines:

- Employees must submit a Request for Change to Work Schedule (see Appendix A) if they want a flexitime schedule.
- The section/division director must make a determination that the request will be in the best interest of the Agency.
- A copy of the request should be forwarded to the HRD for placement in the employee's personnel file.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 16: OFFICE MANAGEMENT

Once the request is approved, no further changes in the employee's work schedule may occur without approval by the section/division director.

Variations in working hours because of irregular workload or deadlines are not to be considered flextime and may result in the recording of compensatory time, thus requiring prior approval of the section/division director.

EXCEPTION: Employees reporting directly to the Secretary of State or the Deputy Secretary of State may work and record less than eight (8) hours for a particular workday, provided the employee works and records the minimum hours required for the work week. However, this practice should be used sparingly and avoided if possible. If fewer hours than required are worked for a particular week, appropriate accrued leave must be used and such use should be reflected on the monthly timesheet.

The section/division director may revoke flextime schedules of employees at any time if the flextime schedules are no longer in the best interest of the Agency.

16.4 TELECOMMUTING

Telecommuting is an arrangement in which an employee works from a location other than the employee's regular or temporarily assigned place of employment. Telecommuting may be available to employees when it would be of mutual benefit to the employee and to the Agency. Telecommuting is not an employee benefit or right. It is based on the Agency's needs and the employee's past and present levels of performance. An employee must obtain approval for a telecommuting request from the Secretary of State/Deputy Secretary of State through the employee's section/division director.

An employee approved for telecommuting may not accrue state compensatory time for work performed at the employee's personal residence.

An employee who does not have a telecommuting arrangement may accrue compensatory time for work performed at the employee's personal residence if the employee obtains advanced approval from the employee's division director or from the Deputy Secretary of State.

16.5 OFFICE DECORUM

Employees are representatives of the Secretary of State. Employees are expected to carry out their duties in a professional manner and maintain the appearance and conduct reflective of this professionalism.

- 1. Dining in Public Areas** - Employees may eat or drink at their workstations not located in a public area provided that the eating does not cause a health hazard, soil or damage the workplace, disrupt office activity, or impair the employee's job performance.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 16: OFFICE MANAGEMENT

2. **Break Areas** - Rooms are available for the use of employees for break periods. Employees should keep these areas neat and clean by discarding wrappers and other trash in the receptacles and cleaning up spills. Refrigerators and microwave ovens should be cleaned at least weekly.
3. **Smoking** - In consideration of the health of Agency employees and visitors, smoking (pipes, cigars, cigarettes, and electronic cigarettes) is prohibited in and within fifteen (15) feet of a public entrance to buildings occupied by Agency employees.
4. **Plants** - Employees may have plants as long as the plants are contained in pots with non-absorbent saucers to avoid making rings on desks or carpets. Plants should be properly maintained and trimmed.
5. **Work Stations** - Personal items at work stations should be kept to a minimum and always in keeping with the professional atmosphere of the Agency. Nothing may be hung from, attached to, or drawn on blinds, ceilings, doors or other such fixtures. Items, including plants, are not to be placed on the modular work stations or components so that the items are visible above the walls of the work station.
6. **Wall Mountings** - Mountings on standard walls inside or outside of offices should be attached with picture hangers, and not tacked, stapled, or taped. Anything hung on a wall or panel should be framed. Only masking tape should be used to mount temporary informational signs and/or posters on building wall surfaces and Agency furnishings. This will protect the surface of the inside and outside of the building and not damage the surfaces. However, any wall hangings desired in the office space located inside the Capitol Building must be approved by the State Preservation Board.
7. **Appliances** - For employee safety and the efficient operation of heating, ventilation, and air conditioning systems, employees may not have personal electric space heaters, heating elements, portable fans, or personal coffee pots unless approved by their section/division director. Under no circumstances should these appliances be plugged into modular furniture outlets. These energy users operate against the central system and defeat its efficient operation and constitute a safety hazard. The use of “low volume” radios or other such devices is permitted as long as the devices are not in public view, cannot be heard over the phone, and do not disturb other employees.
8. **Bulletin Boards** - Bulletin boards are located in each break room. Only official Agency postings are permitted to be on the bulletin boards. Subject to approval by the Human Resources Manager, bulletin boards located in break rooms may be used to post notices concerning buying and selling of personal items and to announce events concerning employee activities or meetings. The posting of literature that appears to conflict with the Agency’s neutral position (e.g., political matter, certain employee organizations, and associations) is prohibited.
9. **Personal Standards of Conduct** - Personal conduct, grooming, and dress of all employees are expected to conform to businesslike standards. Employees should

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 16: OFFICE MANAGEMENT

dress in a manner that is in keeping with the generally accepted standards of office attire.

10. **Personal Business** - Employees should conduct personal business during non-business hours. When a situation necessitates the employee's handling of personal business while at the employee's work station, the employee should make every effort to minimize disruptions to other employees or to members of the public who may be in the general area.
11. **Conference Rooms** - These rooms are to be used for state purposes only. The conference rooms in the Rudder Building may be reserved by contacting the assistant of the division/section in which they are located. Conference rooms in other buildings must normally be reserved through the Texas Facilities Commission. The convener of a meeting is responsible for leaving the rooms neat and orderly. These rooms may not be used as lunch or break areas.
12. **Animals** - An employee is prohibited from bringing animals to the workplace except where they may be permitted by law to bring animals into the workplace, such as may be the case with "assistance animals" used to assist a disabled employee (as defined by Section 121.002, Texas Human Resources Code).

16.6 PROCUREMENT

It is the responsibility of the Purchasing Department (Purchasing) to make all Agency purchases and commitments of any kind regarding services, goods, and equipment and to ensure that such purchases are in compliance with state regulations and Agency policies. One purpose of this policy is to protect the financial and operational interests of the Agency. Following are some of the state purchasing rules and guidelines with which the Agency must comply:

- State contracts are in effect for many items the Agency purchases.
- The Agency is required to give preference in purchasing products and services from TIBH Industries, Inc. (Texas Human Resources Code, Chapter 122).
- A portion of Agency annual expenditures should be contracts or purchases of goods or services from Historically Underutilized Businesses (HUBs)(Texas Government Code, Chapter 2161).
- A minimum of 8 percent of Agency annual purchases of goods are required to be recycled or remanufactured materials.

Purchasing makes commitments to purchase services, goods, and equipment only when based on a properly completed and approved Purchase Requisition (PR). It is improper for anyone other than purchasing personnel to make such commitments or to modify such commitments. Examples of purchasing-related activities that should be handled through the Purchasing Department are:

- Soliciting information from vendors;
- Contracting for telecommunications services;
- Contracting for other services such as training, consulting, or programming;

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 16: OFFICE MANAGEMENT

- Repair or replacement of equipment not covered by a maintenance contract;
- Equipment trade-ins;
- Vendors making cold calls should be referred to Purchasing; and
- Arranging for on-site demonstrations or obtaining products for evaluation.

Section/division directors may initiate product evaluations by informing Purchasing of their intent. After Purchasing indicates its concurrence, if any, the vendor may be contacted for delivery of the product. All correspondence with the vendor must state clearly “evaluation purposes only” and disclaim any contract for purchase. An evaluation period shall not exceed sixty (60) days. Shipping documents or receipts for the product will be submitted to Purchasing. All products received for evaluation will be returned to the vendor; if the section/division director wants to order the product, the regular requisitioning process applies. When the product on loan is returned or picked up, a receipt must be obtained from the vendor and forwarded to Purchasing.

16.7 SEMINARS AND CONFERENCES

All funds collected for the reimbursement of costs directly associated with the conducting of seminars, conferences, or clinics that directly relate to the legal responsibilities and duties of the agency and that are for the purposes of education, training, or informing employees or the general public are hereby appropriated for the necessary expenses incurred in conducting the seminar; provided, however, all applicable laws and rules and regulations for the acquisition of goods and services for the state shall apply to the expenditures.

The Agency shall charge a reasonable registration fee which shall be set at an amount estimated to cover the cost of each seminar or conference conducted. It shall not be the intention of the Agency to profit from the collection of registration fees.

State funds, including registration fees, shall not be expended on alcoholic beverages, entertainment, or promotional items/gifts for attendees.

All seminar/conference-related expenditures shall meet specifically established Agency purchasing and approval requirements.

A site selection bid process shall be used by the Agency. Records shall be kept to verify that a minimum of three (3) bids for each seminar/conference have been solicited. The site selection process shall be based on room rates, availability of sleeping rooms for conference attendees, and meeting space required. Based on the required variables, the hotel with the lowest bid that can meet the minimum requirements of the seminar/conference will be selected.

The Agency will require all invoices from vendors and Banquet Event Order forms approved by Agency personnel to be accurately and completely itemized.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 16: OFFICE MANAGEMENT

All vendors' invoices and other supporting documentation relating to seminars/conferences conducted by the Agency will be attached to vouchers retained in Agency files.

Written procedures, approved by the Administrative Services Division for handling cash receipts, admittance to seminar/conference functions, and reporting on the financial results of each seminar/conference will be followed as stated below:

- A cash receipt log shall be maintained by the applicable division for Agency seminars.
- The cash receipt log shall have the name of each person registering for the seminar, the cash receipt, date, and the amount received.
- Identification badges shall be provided for each participant at the hotel. Each participant's identity shall be verified before the participant receives a badge. If a different individual attends the seminar from the original payee, that attendee must sign next to the payee's name.
- The revenue accountant from Financial Management shall verify the number of badges processed against the revenue received.
- A representative from the applicable division shall notify the hotel as to the guaranteed number of paid attendees. The hotel shall charge for food accordingly. The hotel shall itemize charges for the guaranteed number of each function. If any discrepancies occur, the discrepancies shall be documented and explained to allow reconciliation between the hotel bill and the badges issued. A final reconciliation shall be completed by the revenue accountant the first business day following the seminar.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 17: PERSONNEL MANAGEMENT

17.0 EMPLOYEE PERFORMANCE EVALUATION

The performance evaluation procedure provides criteria for evaluating employees' job performance, work-related conduct, individual improvement plans, and follow-up documentation on individual improvement plans based on job-related functions, agency needs, and consistently applied policies that comply with laws prohibiting employment discrimination. Division/section directors shall review completed evaluations to ensure their division/section is consistently applying evaluation procedures. The HRD will review completed evaluations and evaluation forms annually to ensure compliance with Agency policy, compliance with equal employment opportunity law, and consistency of application throughout the Agency.

Each employee's performance evaluation shall be determined in accordance with objective, job-related, independently measured production expectations and job-related conduct. Job-related conduct is defined as being in compliance with the Agency's policies, procedures, and workplace rules that can be objectively defined, measured, and documented. All performance evaluation ratings shall be supported by a description of conduct that constitutes the basis for rating an employee's performance. Managers/team leaders shall develop an Improvement Plan (IP) when an employee receives a "Needs Improvement" rating. The IP will state the specific skills needing improvement and shall outline a course of action using specific, job-related, and measurable actions. Time frames for planned actions shall also be stated in the IP. Follow-up documentation shall be forwarded to the HRD for placement in the employee's personnel file. Follow-up documentation must also be based on job-related and measurable job performance or job conduct that is consistently applied.

Employee-specific performance objectives shall be established by employees and managers/team leaders with the approval of the division/section director. Specific performance objectives shall be developed using objective, job-related, measurable, and consistently applied criteria.

New employees shall meet with their manager/team leaders to discuss specific performance objectives within four (4) weeks of employment. The manager/team leader will submit to the HRD the new employee's Initial Performance Goals that will become part of the overall performance evaluation plan. After completing each evaluation, managers/team leaders shall develop specific performance objectives for the next evaluation period. When possible, directors will ensure employees' performance evaluation goals are linked to the goals of the Agency's Strategic Plan.

An employee's performance will be assessed by reviewing documented production rates, the ability to meet stated deadlines/turnaround times, comments received from the public and other management personnel, and through personal observance of the employee's performance and job-related conduct.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 17: PERSONNEL MANAGEMENT

Managers/team leaders will complete performance evaluations for any of the following reasons:

- Completion of the first six (6) months of employment using the Orientation Period Employee Appraisal;
- Promotion to a new position; or
- Annual Evaluation (Evaluation period is July 1st through June 30th).

Managers/team leaders may complete performance evaluations for any of the following reasons:

- Evidence that an employee's overall performance is sub-standard based on specific performance objectives established for the employee's position; and
- Upon an employee's request with concurrence of the employee's manager/team leader.

Employee performance evaluations are reviewed before approval of any of the following personnel actions:

- Promotions;
- Merit increases;
- One-time Merits; and
- Reimbursement for tuition pursuant to Texas Government Code Chapter 656, Subchapter C, Training, and Subchapter D, Restrictions on Certain Training.

Employee Appraisals and instructions are in Appendix A. Completed evaluations shall be forwarded to the HRD by July 31st of each year.

17.1 DISCIPLINARY ACTION

Disciplinary actions shall be based on job performance and job-related conduct. Job performance is defined as the employee's ability to perform effectively the functions of the job, based on demonstrated skill as documented by objective, job-related, and measurable criteria that is consistently applied. Job-related conduct is defined as compliance with Agency's policies, procedures, and workplace rules that can be objectively defined, measured, and documented. Methods of assessing an employee's job performance or job-related conduct shall include written documentation, personal observation, statistical documentation, and oral discussions.

The Human Resources Manager shall review all formal counseling reports and disciplinary action reports prior to consulting with an employee to ensure consistency of application and compliance with Agency EEO Plan.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 17: PERSONNEL MANAGEMENT

Although Agency employees serve at the pleasure of the Secretary of State or the Deputy Secretary of State, substandard performance of assigned job duties, job-related conduct prohibited by Agency's policies or procedures, or violations of state or federal laws involving a felony or Class A or B misdemeanor, can result in disciplinary action up to and including termination. Off-the-job personal conduct may be grounds for disciplinary action. Employees who are arrested and charged with a crime may be transferred to another position, assigned different duties, placed on leave without pay, or terminated, at the discretion of the Secretary of State or the Deputy Secretary of State, depending upon

- The nature of the crime(s);
- The effect of the employee's arrest and charging may have on his/her job performance;
- The extent to which the employee's arrest and charge may, if known, diminish public confidence in the Agency; and
- Any other relevant factors.

Employees may be terminated immediately or immediate disciplinary action may be taken in instances approved by the Secretary of State or Deputy Secretary of State. In other situations, the disciplinary procedures discussed in this section shall be followed.

Grounds for Disciplinary Action

Specific job-related performance or conduct that represents grounds for disciplinary action up to and including termination, include, but are not limited to the following:

- Acts of insubordination that involve the refusal to comply with Agency's policies and procedures or supervisory instructions and orders related to the performance of assigned job duties or responsibilities;
- Misuse or theft of Agency funds or property;
- Below-standard performance of assigned job duties or responsibilities;
- Conduct that interferes with the performance of assigned job duties and responsibilities;
- Conduct that violates state or federal laws involving felonies or Class A or B misdemeanors related to the employee's official capacity as an employee, or that adversely impacts the public image of the Agency; and
- Conduct that is prohibited by Agency's policies and procedures.

Procedure for Documentation

Disciplinary action shall be taken in the following manner:

1. The employee's manager along with the employee's team leader shall meet with the employee and inform the employee of performance or conduct problems as well as expected improvements. The manager and team leader may make a written record of the meeting. The written record will not be placed in the employee's personnel file

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 17: PERSONNEL MANAGEMENT

and the employee will not be asked to sign the report. The written record may, however, be attached to any future formal counseling reports.

2. If the employee's performance or conduct does not improve, the employee's manager and team leader shall formally counsel the employee. The manager, team leader, and the employee shall sign a written record of the session. If the employee refuses to sign the written record, the manager and team leader shall request that another manager or team leader confirm that the counseled employee was presented with the written record. The written record shall state the cause for the counseling, the action the employee should take to correct the cause for the counseling, and the timeframe within which the performance or conduct must be corrected. The manager of the HRD shall review the written record before counseling the employee. The Formal Counseling shall be sent to the director of the section/division. The HRD and employee shall receive a copy of the signed Formal Counseling.
3. At the end of the time period specified in step 2 above, the employee's manager and team leader shall counsel the employee again. The manager and team leader shall make a written record of the session, documenting how the employee has corrected the cause for counseling. The manager shall forward a copy of the written documentation to the HRD for placement in the personnel file. If the employee has not corrected the reason(s) for counseling, the division/section director shall counsel the employee and prepare a written report placing the employee on Disciplinary Probation. A Disciplinary Probation report shall be filed in the employee's personnel file, with a copy sent to the division/section director (if applicable) and a copy given to the employee. The Disciplinary Probation report shall contain the same type of information as the Formal Counseling, including a time limit within which the performance or conduct must be corrected, and it shall be signed by the section director and the employee. If a disciplined employee works for a full year without further disciplinary action under this policy, the next failure to meet behavior or performance standards may be treated as a First Occurrence under this policy. However, the Agency may still consider all past disciplinary actions in evaluating the employee.
4. Failure to correct the basis of a Disciplinary Probation within the time period established in step 3 above, continued unsatisfactory performance, or repeated counseling reports (on the same or different subjects) may result in a reduction in salary, suspension without pay, or involuntary termination.

No reduction in salary, suspension without pay, or involuntary termination will take place without the written approval of either the Secretary of State or the Deputy Secretary of State.

Section directors who wish to reduce the salary of, suspend without pay, or involuntarily terminate an employee should so recommend to the applicable division director. If the

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 17: PERSONNEL MANAGEMENT

division director is in agreement with the recommendation, the division director should prepare a written memorandum to the Secretary of State or the Deputy Secretary of State recommending the disciplinary action and stating the reasons why such an action should take place.

An employee may file a grievance concerning disciplinary action as outlined in Section 15.

A reduction in salary involving moving into a lower salary group shall be considered a demotion. The Texas Government Code directs that in cases of demotion, an employee's new duties must change to those of the position in the lower salary group.

17.2 TERMINATION OF EMPLOYMENT

Voluntary Termination

Employees should submit a letter of resignation to the section director with a copy to the division director and HRD. This letter should be submitted at least two (2) weeks prior to the last day that the employee will remain on the payroll exclusive of any additional compensatory time that the employee wishes to use. The letter of resignation should contain:

- A concise statement of the exact reason or reasons for resigning;
- The effective date and time of resignation; and
- A statement indicating whether the effective date and time of resignation are based on utilization of any accrued annual or compensatory leave.

Employees who terminate employment will not be paid for unused annual leave if they are re-employed within 30 days by another state agency that grants annual leave.

Employees who want to remain on the payroll to deplete accrued compensatory leave must request approval by completing the "Use of Compensatory Leave" form that states:

- The employee understands that the use of compensatory leave is at the discretion of the employee's division/section director and the Agency.
- The employee understands that the use of compensatory leave will not be considered for an employee who fails to give the required two-week notice prior to the date that the employee wishes to begin using accrued compensatory leave.
- If the employee remains on the payroll using accrued compensatory leave and the employee accepts employment with any other employer (government or private), the employee must notify the HRD and the remaining compensatory leave balance will be lost.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 17: PERSONNEL MANAGEMENT

Once an employee submits a letter of resignation, the employee may not rescind the letter of resignation without approval by the employee's section/division director.

Job Abandonment

Consecutive absences of three (or more) workdays will be considered as job abandonment and will result in voluntary termination if - prior to the end of the employee's third scheduled work day - the employee does not contact his or her manager/team leader in accordance with agency procedures.

17.3 INVOLUNTARY TERMINATION

Employees may be involuntarily terminated in accordance with the procedures set forth in Section 17.1, DISCIPLINARY ACTION. In situations approved by the Secretary of State or Deputy Secretary of State, an employee's employment may be terminated immediately.

Reduction in Force (RIF) - Recall Procedures

Budgetary restrictions, legislative actions, or reorganization may require reductions in the size of the Agency's workforce from time to time. Such RIF may be achieved by the restriction of posted job vacancies and reclassification and reassignment of employees to lower grade positions. If it is not feasible to achieve the RIF by the methods stated above, termination of employees may be considered. The basis for a RIF or recall shall be objective, job related, and consistently applied.

The Secretary of State or the Deputy Secretary of State, the affected division director, the Director of Administrative Services, and the Human Resources Manager shall confer regarding any anticipated RIF or recall. If the Secretary of State or the Deputy Secretary of State decides to reduce the workforce, the division director shall inform the section director being affected and request recommendations for positions to be deleted. The division director, the Director of Administration, and the Human Resources Manager shall review the implementation of RIF criteria to ensure consistency of application.

In cases where duties are to be consolidated and individual positions deleted or where positions requiring higher level or different skills are to be created, job performance, necessity of the functions of the job, veteran's preference, and seniority shall determine the employee(s) to be retained. "Job performance" is defined as an employee's ability to effectively perform the functions of the job based on demonstrated job skills.

Managers shall review each employee's performance appraisals and shall base their recommendations to the section director and division director on past and current job performance, necessity of the functions of the job, veteran's preference, and seniority. These criteria shall be independently quantified on the basis of a numerical score. Each employee subjected to a RIF or recall within a given job classification and organizational unit should be given a score for each of the four criteria. The decision as to which

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 17: PERSONNEL MANAGEMENT

employees are to be laid off shall be based on the total combined score of the four criteria. The employees with the lowest total score shall be subject to layoff.

The Secretary of State or the Deputy Secretary of State shall review the recommendations and justifications submitted by the division director. The final decision shall be made by the Secretary of State or the Deputy Secretary of State. The section/division director shall inform the affected employees. Employees terminated through a RIF shall be given notice of impending actions as far in advance as practicably reasonable.

An employee shall be allowed to remain on the payroll while using all accrued compensatory time and shall receive a lump sum payment for any accrued annual leave upon termination from state employment, provided that the employee is not re-employed within thirty (30) days from the date of termination by a state agency that grants annual leave. Employees that are eligible for a lump sum payment shall be paid 45 days from the date of termination.

Employees terminated from employment with the state under a formal RIF policy shall have their sick leave balance restored if they are re-employed by the state within twelve (12) months of their separation.

If time and budgetary constraints allow, employees shall be offered job skills training courses to help with their job-seeking efforts. The Administrative Service Division shall coordinate this effort with the employee.

17.4 EXIT INTERVIEW

Employees who terminate employment must have an Exit Interview with the HRD. The HRD shall ensure that terminating employees:

- Complete all required paperwork concerning Agency-assigned property, pay, leave, and benefits; and
- Receive an opportunity to complete the State of Texas Employee Exit Survey.

Final warrants will not be released by the Financial Management Section until the HRD confirms that an Exit Interview has been conducted.

17.5 MULTIPLE EMPLOYMENT WITH THE STATE

Employees who are legally employed with another state agency are subject to the following provisions:

- Separate leave records must be maintained for each position.
- State service credit will accrue as if the employee had a single position.
- Leave balances do not transfer upon termination of one position.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 17: PERSONNEL MANAGEMENT

- State contribution toward the employee's benefit replacement pay will be subject to the overall individual limits.
- State contribution toward the employee's group insurance is limited to the amount specified for a full-time active employee.
- The employee must notify his or her employer prior to accepting a second position.
- In the case of FLSA-non-exempt positions, both employers must coordinate with each other to ensure that the employee is appropriately paid for working more than 40 hours in a workweek.

17.6 ARREST, CHARGING AND/OR CONVICTION OF AGENCY PERSONNEL

Similar to its policy regarding the hiring of persons with a criminal record, the Agency's policy regarding the arrest, charging, and/or conviction of employees is intended, among other things, to provide a crime-free work environment and to produce a law-abiding workforce.

- An employee who is arrested and charged with any offense, other than a misdemeanor traffic violation, must notify the employee's manager/team leader in writing within one (1) business day of the date of the arrest, stating the date of the arrest and the charge. Failure to comply with this policy is considered misconduct and may result in dismissal. The manager/team leader so notified shall immediately notify the manager's section/division director and the Deputy Secretary of State.
- An employee who is arrested and charged with a crime or crimes may be transferred to another position, assigned different duties, placed on leave without pay, or terminated at the discretion of the Secretary of State depending upon:
 - The nature of the crime(s);
 - The effect that the employee's arrest and charging may have on his/her job performance;
 - The extent to which the employee's arrest and charging may, if known, diminish public confidence in the Agency; and
 - Any other relevant factors.

17.7 EMPLOYMENT REFERENCE CHECKS/VERIFICATION OF EMPLOYMENT

All requests for references or verifications of past or present employment history shall be referred to HRD. Employees are not authorized to comment on other employees' (past or present) work history, job performance, or eligibility for re-hire.

17.8 CHANGES IN PERSONAL INFORMATION

Employees should promptly initiate any changes in name, address, or telephone number using ERS Online.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 17: PERSONNEL MANAGEMENT

The Texas Public Information Act states that employees may elect to disclose or prohibit public disclosure of their home address, telephone number, social security number, information about family members or emergency contact information.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 18: BUILDING MANAGEMENT

18.0 EMERGENCY PROCEDURES

In Case of Fire

1. Immediately set off the fire alarm.
2. Evacuate the building.
3. Dial 9-911.
4. Contact Capitol Security at 3-3333.
5. Contact the Deputy Secretary of State at 3-5702.

In Case of a Bomb Threat

1. Try to obtain as much information as possible from the caller, e.g., where the bomb is located, when it will explode, what kind of bomb it is, the caller's name, and the caller's address.
2. Immediately set off the fire alarm.
3. Evacuate the building.
4. Contact Capitol Security at 3-3333.
5. Contact the Deputy Secretary of State at 3-5702.
6. Report to Capitol Security everything from the phone conversation that might help apprehend the caller, e.g., distinctive voice, background sounds, and threat language (well-spoken, foul, incoherent, etc.).

In Case of a Medical Emergency

1. Immediately dial 9-911
2. Contact the HRD.
3. In the event of serious injury to or the death of an employee, do not contact anyone in the employee's family. Refer all telephone calls to the HRD.

18.1 SAFETY SYSTEMS

All Agency buildings are equipped with safety devices such as fire extinguishers, smoke detectors, and automated fire alarms. While the built-in safety features can give employees a sense of security, employees also need to take sensible safety precautions. Accidents can occur from the stacking of files, furniture, boxes, and other materials around work areas, in the corridors, and in aisles.

18.2 SECURITY

The HRD issues each employee an Electronic Access Card (EAC). The Texas Department of Public Safety laminates the agency's name, employee's name, and employee's photo on the EAC and is responsible for programming the clearance code(s) to the EAC. The clearance code limits access to designated buildings and offices during business and non-business days and hours. The EAC must be visible at all times. Employees who need, forget, or lose an EAC must contact the HRD.

Each section/division is responsible for unlocking the door(s) to its office in the morning. Security officers check for locked doors during night patrols. Employees working late at

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 18: BUILDING MANAGEMENT

night may call Capitol Security at 3-3556 for an escort to their automobiles when they are ready to leave the buildings.

The Purchasing Department maintains control over the issuance of keys. Keys shall be issued only after approval by the section/division director. Employees sign for acceptance of the keys and assume responsibility for the key's safekeeping. Keys assigned to an employee should not be shared or relinquished to another employee; the key must be re-issued by the Purchasing Department. Any changes to locks shall be accomplished by written request from the section/division director.

18.3 SIGNS

Agency buildings are equipped with building directories and signs designating each office and department. The Secretary of State or the Deputy Secretary of State must approve any changes to the signs.

18.4 OUTSIDE OR NON-PROFIT ORGANIZATIONS

Solicitation, the selling of items and goods, fund-raising projects, or the placement of commercial advertisements inside Agency buildings or offices is prohibited at all times, by employees and non-employees, with the following exceptions:

Solicitations for non-profit organizations that are conducted on behalf of the Agency have been limited by the Legislature to the annual State Employee Charitable Campaign (SECC) that covers over 200 charitable organizations. Employees shall not be required to contribute or be coerced into contributing. Such solicitations are to be conducted in a professional and orderly manner so as to entail minimal distraction of employees from their duties.

18.5 SOLICITATIONS REQUESTED BY OFFICE OF THE SECRETARY OF STATE (GOVT. CODE 405.005)

The Secretary of State shall review and approve all plans or efforts to solicit or accept gifts, grants, or other donations, including in-kind contributions, prior to such solicitation or acceptance.

Gifts, grants, and donations may be solicited and/or accepted only for a lawful purpose related to the purpose of the Office of the Secretary of State.

Employees authorized to solicit or accept gifts, grants, or donations shall provide a Request for Approval for Gifts, Grants or Other Donations to the potential donor for completion and ensure completion of said form by the donor. A copy of the completed form shall promptly be submitted by such employees to the Director for Administrative Services for inclusion with other financial records.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 18: BUILDING MANAGEMENT

Any money donated to the Office of the Secretary of State shall promptly be deposited in the Treasury. Expenditures of funds donated to the Agency must meet Agency purchasing and approval requirements.

18.6 MODIFICATIONS TO BUILDINGS OR OFFICES

Any modifications to buildings or offices must be approved in advance by the Secretary of State or the Deputy Secretary of State.

18.7 BUILDING MAINTENANCE

The Texas Facilities Commission (TFC) is responsible for maintenance of Agency-occupied buildings. Maintenance includes temperature control, plumbing, custodial services, changing of lights, and other such services. Employees should do their part to maintain a clean and orderly work environment. Employees should report building maintenance problems to their section/division director or to their section/division directors' designees. The section/division directors will contact the Purchasing Department. The Purchasing Department will report the problem(s) to the TFC via TFC's web portal. The Purchasing Department will send a copy of the confirmation receipt from TFC to the section/division director. Building maintenance problems in the Capitol Building should be reported to the State Preservation Board.

18.9 ACCIDENT PREVENTION PROGRAM

The Agency regards its employees as its most valuable asset. In accordance with Executive Order GWB-95-8, personal safety and safe practices in the workplace shall be emphasized on a regular basis. It is the Agency's goal to prevent avoidable accidents and injuries.

The responsibility for the administration of the Accident Prevention Program is assigned to the Agency's Safety Officer and a Safety Committee appointed by the Secretary of State or Deputy Secretary of State. The Safety Officer serves as chairperson of the Safety Committee. The responsibilities of the Safety Committee are to promote accident awareness throughout the Agency and to heighten employee interest and involvement through quarterly safety inspections, occasional films and lectures, and professional training in emergency first aid, CPR/AED, and related topics.

Managers at all levels play an important role in the Accident Prevention Program. Managers and team leaders shall incorporate safety as an integral part of all programs and observe the safety regulations of the Safety Committee.

Employees are responsible for practicing safe working habits and for following the safety regulations set out in the Agency's safety program. Employees are encouraged to offer suggestions to their team leaders, Safety Committee members, and the Agency Safety Officer as to how to keep themselves and their coworkers, and their work areas safe.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 18: BUILDING MANAGEMENT

It is the intent of the Agency to achieve maximum compliance with safety procedures and regulations established by the State Office of Risk Management (SORM).

Employees must contact their team leader and the Workers' Compensation Claims Coordinator if they sustain an injury or illness, no matter how small, during the course and scope of performing their job duties. The Workers' Compensation Claims Coordinator will file a DWC-1S (Employer's First Report of Injury or Illness). The injured employee must file a SORM-29 (Employee's Report of Injury or Illness). Witnesses, if any, to the accident must complete a SORM-74 (Witness Statement). The Workers' Compensation Claims Coordinator will submit all forms and any other information regarding the accident to the SORM. The Agency Safety Officer shall investigate the accident and try to eliminate the possibility of recurrence.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 19: TRAVEL

19.0 TRAVEL POLICIES AND PROCEDURES

The Office of the Secretary of State travel policies and procedures are in compliance with the Texas Comptroller of Public Accounts travel policies and procedures. The Comptroller's Office developed the [Textravel](#) website which is based on [Texas Government Code Chapter 660, General Appropriations Act, Article IX, Part 5](#) , and [Texas Administrative Code, Title 34, Part 1, Chapter 5, Subchapter C, Section 5.22](#).

Our agency has developed agency policies and procedures to further ensure proper internal control and conservation of state funds.

19.1 TRAVEL REQUESTS

All official travel must be approved in advance by the Secretary of State or the Deputy Secretary of State, the Director of Administrative Services, and the director of the division to which the employee is assigned. A *state agency* may only pay for business-related travel expenses incurred outside of Texas if the travel was approved in advance in accordance with the policy of that agency. [Texas Government Code Section 660.003\(e\)\(4\)](#). An online travel authorization request via the [Travel Authorization System](#) must be submitted by the employee to his or her division director. First time travelers will need to contact Travel Administration in the Financial Management Section to have a travel account setup. Travel Administration will then contact the Agency security coordinator to set up a User ID and a password.

The employee should not arrange for transportation and lodging reservations before his/her travel request has been approved via the online Travel Authorization System.

After the travel request has been submitted online, the employee's division director will be notified through an email message. The request will be reviewed and considered for approval by the employee's division director.

If the request has been approved by the division director, the Director for Administrative Services will review the request. If the request is approved by the Director for Administrative Services, the Deputy Secretary of State will review the request and make the final determination. .

In the case that the employee seeking approval for official travel is a division director, the Director for Administrative Services, and subsequently the Deputy Secretary of State, will review the request for approval.

If the traveler is the Director for Administrative Services, the Deputy Secretary of State will review the request for final approval.

The Deputy Secretary of State makes the final determination of approval in the Travel Authorization System. The Secretary of State and the Deputy Secretary of State are not required to seek prior approval in the Travel Authorization System for their own official

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 19: TRAVEL

travel. The Deputy Secretary of State also gives final approval for all official travel in the Executive Division.

Election Inspectors

The Office of the Secretary of State has the statutory duty to appoint one or more state inspectors for an election, Texas Election Code, Title 3, Chapter 34. The Director of Election Administration approves the recruitment, appointment, and training of state election inspectors. No further approval is required by the Director of Election Administration in the Travel Authorization System for election inspector travels. The Director of Election Administration or his/her designee will also supply a list of employees recruited from other agencies, if any, to the Financial Management Section.

If the election inspector is a Secretary of State employee, the travel will be approved in the Travel Authorization System by the employee's division director, the Director of Administrative Services, and finally the Deputy Secretary of State.

If the election inspector is an employee from another state agency, Travel Administration will determine if the person has an established travel account. If not the Travel Administration will set up an account in the Travel Authorization System and contact the Agency security coordinator for proper security password setup for the individual. The travel will be approved in the Travel Authorization System by the Director of Administrative Services and finally the Deputy Secretary of State.

19.2 ADVANCE TRAVEL PAYMENTS

Advance travel payments may be requested for statutorily mandated travel, such as election inspections. Other employees may also request advance travel payments by documenting a need through the online [Travel Authorization System](#). The Director for Administrative Services may approve or reject any advance travel payment requests.

The Agency will advance funds to employees for projected travel expenses only if the expenses are incurred during travel that requires an overnight stay outside of the employee's designated headquarters. Any exceptions will need to be approved by the Director for Administrative Services.

A travel voucher must have been submitted documenting the use of advance travel funds before another advance for subsequent travel may be issued. Unused Advance Travel Funds are due to the Agency three (3) days after the travel voucher has been submitted to Financial Management. All outstanding balances should be cleared, within thirty (30) days after completion of the travel.

The advance travel account shall not be used to reimburse any employee after the travel has occurred.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 19: TRAVEL

19.3 MULTIPLE ADVANCES OR REIMBURSEMENTS FOR A TRAVEL EXPENSE

A state employee may not accept a reimbursement or advance for a travel expense from more than one source. A state employee who anticipates receiving or actually receives a reimbursement or advance for a travel expense from a person or organization other than a state agency may seek an advance or reimbursement for the expense from a state agency only to the extent that the amount of the employee's advance or reimbursement from the other person or organization is less than the amount of the total expense incurred.

19.4 TRAVEL VOUCHER DOCUMENTATION REQUIREMENTS

The supporting documentation for a travel expense must provide sufficient detail or justification to demonstrate that:

- An expense was incurred while conducting official state business; and
- The activities engaged in while traveling were necessary to conduct official state business;
- Travel was necessary to conduct official state business.
- The supporting documentation required by the voucher and documentation requirements must be made available to the Comptroller and the State Auditor.
- For voucher and documentation requirements, "travel expenses" includes a registration fee or tuition paid to attend a seminar.

19.5 MULTIPLE EMPLOYEE TRAVEL

If more than one employee is traveling and incurs expenses for the same or similar official state business, the supporting documentation for those expenses must provide sufficient detail or justification to demonstrate it was necessary for more than one employee to travel. To conserve state funds Managers should minimize the number of people who travel to the same seminar, conference, or event.

Coordination of Travel

If two or more employees are traveling to the same destination by personal vehicle, the employees must travel in a single vehicle unless the manager/team leader of an employee determines that this arrangement is not feasible or preferable for that employee.

19.6 ATTENDANCE AT SEMINARS AND CONFERENCES

Except in those circumstances deemed by a Division Director or the Deputy Secretary of State to make timely provision impossible or impracticable, travel requests to attend seminars and conferences must be received in the Administrative Services Division thirty (30) days in advance of the departure date.

A travel request via the [Travel Authorization System](#) must include all costs, including registration fees, for attending seminars and conferences. Additionally, the travel request must comply with the following requirements:

- An agenda or course outline must be attached to each travel request.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 19: TRAVEL

- The statement of purpose of the travel must directly correlate to statutory duties and agency goals, objectives and strategies.
- A concise statement of the benefit to the state must be included.
- Acronyms should not be used.

Managers should minimize the number of people who travel to the same seminar, conference, or event, to conserve state funds.

19.7 REIMBURSEMENT OF TRAVEL EXPENSES

When employees are requested to speak, present seminars, or otherwise impart information in their area of expertise and doing so is related to the duties of the Agency and advances the State's interests, employees may, on approval, seek and accept reimbursement or in-kind contributions from the outside parties for any travel costs to conserve state funds. In this instance, a travel request should be submitted indicating that travel expenses will be reimbursed by the sponsor. Reimbursements for travel expenses should be made payable to the state. Direct payments should not be made to an employee.

19.8 REIMBURSEMENT OF GASOLINE COST

Gas station receipts showing price per gallon and number of gallons purchased are required for reimbursement purposes. When store receipts are missing or unavailable, a copy of a credit card statement or debit card statement issued by a financial institution is acceptable. The transactions of the purchases need to be clearly identified and marked on the copy of the statement. The traveler also needs to affirm that the amount shown on the transactions were for gasoline purchases only. Other items purchased at the gas station may or may not be reimbursable. Food items purchased at the gas station may be reimbursable but need to be reported on a meal expense form instead. Gasoline cost claims without the above documents cannot exceed a calculated limit. The limit is determined by a formula based on the approximate gas price shown on <http://austingasprices.com> (or comparable website) on the days of travel, the number of miles driven and 25 miles per gallon for standard size cars. Gas mileage reimbursement rate might vary for larger size cars.

19.9 TRANSPORTATION ALLOWANCE

Airfare

Texas Government Code Section 660.093 states that "The amount that a state agency pays or reimburses for a state employee to travel between points by commercial airline may not exceed the lowest rate available." Since state employees may not have the resources to research and find the lowest rate available, state-contracted travel agencies are in a much better position to do this. The agency traveler should request airline tickets from the state-contracted vendor (travel agency) which will bill the cost of the airline

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 19: TRAVEL

tickets directly to the Agency. In the event of schedule changes or other unforeseen circumstances, employees may purchase airline tickets directly from a state-contracted airline and pay the airfare from personal funds. A receipt must be attached to the travel voucher to obtain reimbursement for airfare.

Note: Documentation such as credit card receipt or billing statement, is required for baggage fee reimbursement.

The current state contracted travel agency is:

National Travel Systems

Phone Numbers: (877) 717-7768, (800) 542-0452, (800) 891-9002

Email address : gov@nationaltravelsystems.com

Online booking link : <http://www.nationaltravelsystems.com/state/welcome.html>

Rental Vehicles

Employees must share rental vehicles whenever practicable. Employees must use state-contracted vendors when renting a vehicle unless allowable exceptions exist.

- Employees must make a proper deduction or reimbursement whenever there is personal use of a rental vehicle.
- Rental vehicles should be filled with gasoline when returned.
- One-way rentals resulting in a “drop off” charge should be avoided except in extraordinary circumstances.
- The rental of luxury vehicles must be avoided, except in special circumstances requiring the use of larger vehicles, e.g., several employees traveling together.

The current state contracted rental car vendors are:

Avis Rent A Car System, Inc.

Enterprise Rent-A-Car

Enterprise Rent-A-Car has developed a customized booking tool for our agency at the following link

http://www.enterprise.com/car_rental/deeplinkmap.do?bid=028&refId=TXSECST

When completing the online rental car reservation, a traveler is required to enter a “Travel Authorization #.” This number to be entered is the same Travel Authorization number that was assigned to the travel request in the Travel Authorization System. The traveler will also need to make sure to choose the option of “Secretary of State – Direct Bill” at the welcome page of the customized Enterprise website.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 19: TRAVEL

If the traveler chooses to reserve a rental car with Avis, he or she will need to contact Financial Management to obtain an Avis car rental voucher. Avis requires a preprinted car rental voucher to complete the car rental for state travel.

Travel by Personal Car

It may be more cost effective to rent a car than use a personal vehicle for some road trips. In addition, the State of Texas Business Use Rates offered by the state-contracted rental car vendors include Damage Waiver (DW) and Supplemental Liability Protection (SLP).

Approval in advance by the Executive Division is required if the traveler chooses to use his or her personal vehicle and to seek mileage reimbursement. Reimbursement for the use of personal vehicles is made at the rate listed on the meal and lodging rates webpage.

The traveler must keep track of mileage by using the odometer reading or by using MapQuest electronic mapping system. Point-to-point mileage must be recorded in the Personal Car Mileage Report form. A physical address is required for each point-to-point basis (i.e., FROM: Precinct 1, 123 Monopoly Avenue, Houston, TX – TO: Precinct 2, 2301 Main, Houston, TX).

The state does not reimburse for variances due to being lost or for personal miles (visiting relatives, sight-seeing, etc.) driven while on a business trip.

Travel Between a Residence and the Airport

- An employee driving from his or her residence to the nearest airport may be reimbursed for mileage at the standard mileage.
- An employee may be reimbursed for the mileage incurred by another person while transporting the employee between his residence and the nearest airport during working or non-working hours, so long as the employee demonstrates that the reimbursement would be less than the cost of parking a personally owned or leased motor vehicle at the airport.

Travel Under Special Circumstances

Employees who are away from headquarters on personal leave may be reimbursed for the cost of transportation for returning to headquarters when required to do so by the Secretary of State or the Deputy Secretary of State.

Taxi Fare

The actual cost of taxi fare from Agency headquarters to the airport and from the airport to headquarters is reimbursable.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 19: TRAVEL

19.10 MEALS AND LODGING

Overnight Meals and Lodging

The traveler should wait to reserve lodging until after his or her travel request has been approved. Travelers should reserve lodging through state-contracted properties. A [Hotel Directory Listings](#) has been developed and is maintained by the Office of the Comptroller of Public Accounts.

[Meal and lodging rates](#) differ depending on locations. A traveler must claim the actual expenses incurred for meals and lodging, not to exceed the maximum allowable rates. The maximum should not be claimed unless the actual expenditures equal or exceed the maximum allowable rate.

To conserve state funds, the Agency has further limited the maximum allowable rate for the first day as well as the last day of travel. An interactive overnight meal worksheet in Excel format has been developed to automatically calculate the reimbursable rate for the first and last day of travel.

The calculations are shown in the table below:

First Day of Travel	Reimbursement	Last Day of Travel	Reimbursement
<i>Depart from Headquarters</i>		<i>Return to Headquarters</i>	
Earlier than 7:00 am	100%	7:00 am or earlier	not reimbursable
7:00 am though 11:59 am	75%	7:01 am through 12:00 noon	25%
12:00 noon through 6:59 pm	50%	12:01 pm through 7:00 pm	50%
7:00 pm or later	not reimbursable	7:01 pm or later	100%

The methodology and formula in calculating these limitations were developed by the Director of Financial Management and approved by the Director of Administrative Services.

When making reservations or registering for lodging, employees should use hotels listed on the state contract, if available, and request the State of Texas government rate as listed at [Hotel Directory Listings](#) developed and maintained by the Office of the Comptroller of Public Accounts.

Non-Overnight Meals

The Agency does not reimburse non-overnight meal expenses.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 19: TRAVEL

Actual Expenses

An employee may be reimbursed for actual expenses for meals and lodging when the employee travels with the Secretary of State or Deputy Secretary of State or when the Secretary of State designates a single employee to represent the Secretary of State at a meeting or conference, per Government Code Section 660.206(a) or Section 660.206(b). The request for actual expenses must be made in advance on the Travel Request.

Conservation of State Funds

When conditions warrant, the Secretary of State or Deputy Secretary of State may conserve funds by authorizing less than the maximum rate for reimbursements for meals or lodging expenses. However, an employee shall be notified in advance of travel of any reduction in the reimbursement rates.

19.11 STATE BUSINESS CALLS ON PERSONAL CELL PHONES

Reimbursement for state business calls on personal cell phones is limited to the actual incremental out-of-pocket cost to the traveler (i.e., if the calls did not result in any additional cost to the traveler above the basic monthly rate, there would be no reimbursement). The employee must submit a copy of the cell phone bill with the travel claim with the state business purpose calls marked.

19.12 TRAVEL CONTRACT RESTRICTIONS

Employees must plan travel to achieve maximum economy and efficiency. Employees may be reimbursed for travel expenses only in accordance with the provisions of the current General Appropriations Act, the Travel Regulations Act as amended, the State Travel Management Program (STMP), and the internal procedures of the Agency.

State agencies in the Executive Branch of state government are required to participate in the STMP by using the contracts for travel services awarded by the Comptroller of Public Accounts. These contracts include travel agencies, charge card services, rental car companies, airlines, and hotels.

The contracts listed in the Texas State Travel Directory published by the Texas Comptroller of Public Accounts are available on that agency's website at <http://www.cpa.state.tx.us/procurement/prog/stmp/> and must be used unless an approved exception condition exists. When a contract travel vendor is not used, or when the purchase or reimbursement for airline or rental car transportation exceeds the contract airfare or rental care rate, one of the allowable exception conditions must exist and must appear on the travel voucher or be included with the payment voucher submitted to the Texas Comptroller of Public Accounts.

Allowable exceptions are as follows:

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 19: TRAVEL

- Contract travel agency alternative. Use of an authorized alternative method is allowable if the employee is already in travel status, rendering the use of a contract travel agency impractical or unnecessary, airline reservations are not required, or travel is undertaken as part of a group program for which reservations must be made through a specified source to obtain a particular rate and/or service.
- Lower total cost to the state. Use of a non-contract travel vendor is allowable if the non-contract fare is less than the contract fare and the use of the non-contract vendor results in a lower total overall cost to the State when all trip expenses are evaluated, including ground transportation, insurance fees, parking fees, taxes, and travel time. If the contract travel vendor offers the same, or lower, fare or rate, the contract travel vendor must be used unless a valid exception exists.
- Efficient use of services. Use of a non-contract travel vendor is allowable if necessary because the contract travel vendor is sold out, is not able to provide services at the time or location necessary to accomplish the purpose of the trip, has a real or anticipated labor disruption, or is providing negotiated rates for group travel.
- Health and safety issues. Use of a non-contract travel vendor may be allowed when an employee determines that the accommodations provided by the contract vendor may present a risk to the employee or person under the State's custody in the following circumstances:
 - Accommodations may lack a reasonable amount of security or safety and/or may present a health risk based on the state traveler's individual needs;
 - Accommodations fail to provide an adequate amount of services required for a person with disabilities; or
 - Accommodations have a limited availability of medical emergency facilities or equipment that may be required by a state traveler or person under the state's custody.
- Corporate travel charge card alternative. Use of personal charge cards is allowable only for non-contract airfares used in accordance with this policy if it offers issuance benefits not available from the State's corporate travel charge card contract.

19.13 TRAVEL DISCOUNTS

Employees shall seek and obtain applicable discounts for transportation, lodging, car rental, and other expenses for state business-related travel. Employees are prohibited from accepting state business-related travel discounts when they are traveling on personal business. When an employee is traveling on personal business and a vendor or merchant offers a personal business discount to the employee, the employee may accept such discounts for personal expenses. However, no employee may accept a discount applicable only to state-related business for expenses incurred on personal business.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 19: TRAVEL

19.14 INCIDENTAL EXPENSES

Incidental expenses such as toll fees and parking fees are allowable; however, receipts are required for reimbursement. In addition, the reimbursable parking fee for Austin-Bergstrom International Airport is limited to \$7.00 per day.

19.15 ELECTION INSPECTING

In accordance with Section 34.001 of the Elections Code, the Elections Division is responsible for sending Election Inspectors when the Agency receives a request from fifteen (15) registered voters in the political subdivision conducting an election. To support the mission to ensure the proper conduct of elections, employees must adhere to the following rules:

1. Section Directors will receive an e-mail from the Director of Election Administration requesting volunteers to serve as Election Inspectors. Employees must not contact the Elections Division prior to receiving the request for volunteers.
2. An employee must obtain approval from the Section Director prior to contacting the Elections Division. The employee must specify the amount of time they will be away from the office.
3. The employee must be certified by the Elections Division before serving as an Election Inspector. An employee must attend a training class and receive a passing score to be certified as an Election Inspector.
4. Inspection assignments are based on the needs and requirements of the Elections Division; however, request for specific assignments will be considered. Volunteers are not guaranteed an assignment. Assignments are based on the needs or requests from registered voters.
5. Employees must conform to the agency's travel procedures and submit the proper documentation to the Financial Management Section accurately and as expeditiously as possible.
6. After service as an election inspector, employees must promptly submit an inspection report to the Elections Division.

19.16 ELECTION INSPECTORS NOT EMPLOYEES OF THE AGENCY BUT ARE WORKING ON BEHALF OF THE AGENCY

Travelers such as Election Inspectors from other agencies are subject to the same stringent rules imposed on our Agency travelers. To comply with Texas Election Code, Title 3, Chapter 34, our Agency may need to recruit, train, and appoint employees from other agencies as Election Inspectors. Details of control have been explained in Section 19.1, TRAVEL REQUEST

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 19: TRAVEL

19.17 TRAVEL VOUCHERS

In State Travel

The traveler may enter “In-State” travel expenses into the Travel Claim System, and print and sign the travel voucher within five (5) business days after completion of the travel. The traveler will also need to attach all required receipts to the voucher and forward it to the Financial Management Section. Alternatively, if the traveler does not enter the claim into the Travel Claim System, he or she may submit all required receipts and information to the Financial Management Section, and prepare the travel voucher, print and send it to the traveler for signature.

Out of State Travel

For Out-Of-State travels, the traveler may review and submit the travel claim checklist with all required receipts attached in a timely manner. Financial Management Section will prepare, print, and send (via electronic or traditional mail) the travel voucher to the traveler for a signature. The traveler will need to send (via electronic or traditional mail) the signed voucher back to the Financial Management Section for travel claim processing.

Required Receipt

Receipts are not required for expenses on meals.

However, the following receipts are required:

- Lodging - check-out document reflecting zero balance due.
 - Gasoline purchased for rental car (prepaid receipts need to have gallons and price of gasoline).
 - Parking fees incurred for your personal vehicle or car rental.
 - Taxi fares - date, destination, and amount.
 - Rental car - rental car contract or receipt issued by car rental agency upon return of car showing mileage driven.
 - Airfare - copy of ticket or boarding pass, if available.
 - Baggage fee receipt or credit card statement/receipt.
 - Cell Phone - copy of cell phone bill with state business purpose calls marked
- Other miscellaneous incidental expenses, such as tolls, fax machine use, maps, pens, pencils, etc.

19.18 OMBUDSPERSON DAILY TRAVEL

The Secretary of State’s ombudsperson program is a central part of the Agency’s initiatives to assist needy Texans living in colonias. The program is helping to provide better roads, bring water and wastewater infrastructure to areas that lack these basic services, and improve the quality of life for some of Texas’ neediest citizens.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 19: TRAVEL

If the traveler chooses to reserve a rental car with Avis, he or she will need to contact Financial Management to obtain an Avis car rental voucher. Avis requires a preprinted rental car voucher to complete the car rental for state travel.

Ombudspersons are required to keep an electronic log detailing for each trip:

- Date and time of driving;
- Purpose of the trip;
- Physical address of point of origin;
- Physical address of destination;
- Beginning of odometer reading;
- Ending of odometer reading; and
- Total miles driven.

Ombudsperson Monthly Mileage Report

Each ombudsperson signs and submits electronically a monthly mileage report (the log) to the Director of Colonias. The Director of Colonias will review and approve the ombudsperson's monthly mileage report with his/her signature attached. After the approval, the system will generate a notification email to Financial Management and will prepare a payment voucher and electronically send it to the ombudsperson for signature. Financial Management will proceed with the payment process to reimburse the ombudsperson once the signed copy of the payment voucher is received.

19.19 DIRECT BILLING

State contracted rental car companies and travel agencies bill or invoice our agency directly. Invoices of rental cars and airline tickets will be sent to Financial Management directly through USPS mail, email or fax. The expenditure staff at Financial Management will review the invoices and reconcile them with the travel voucher prepared by the travelers before putting them through the payment process.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 20: HIV/AIDS WORKPLACE GUIDELINES

20.0 PURPOSE

The Agency has adopted the following HIV/AIDS Workplace Guidelines patterned after the model workplace guidelines adopted by the Texas Department of State Health Services.

20.1 POLICY

The Agency shall not discriminate against an applicant or employee on the basis of HIV/AIDS status. The Agency shall give the same consideration and provide the same level of service to individuals of the general public with HIV/AIDS as it does to those without HIV/AIDS.

Current medical research and scientific opinion indicates that there is no risk of HIV/AIDS transmission in the normal work setting. Routine daily encounters with co-workers pose no risk of transmitting the fragile blood-borne HIV/AIDS virus.

Following is a summary of the guidelines:

- No individual, either non-employee (applicants for employment and the general public) or employee, with HIV/AIDS shall be discriminated against in any manner, or excluded from employment, assignment, training, increased compensation, or privileges of employment on account of having HIV/AIDS.
- Neither non-employees seeking employment with the Agency nor employees with HIV/AIDS shall be classified or segregated in any way that would deprive them of equal employment opportunity or adversely affect their status as an employee.
- An employee with HIV/AIDS is entitled to the same rights, privileges, and opportunities, and is governed by the same policies, as any other employee with any other chronic, potentially limiting, or life-threatening illness or other communicable disease.

20.2 CONFIDENTIALITY

Before symptoms occur, an employee with HIV/AIDS is not obligated to provide HIV status information. As with other illnesses, once HIV/AIDS related symptoms occur, it is the employee's responsibility to follow the requirements set forth in Section 9 (General and Miscellaneous Leave) and Section 21 (Americans With Disabilities Act).

Any medical documentation or information provided to management personnel (employee's section/division director, Deputy Secretary of State, and Secretary of State) by an HIV/AIDS infected employee is considered confidential and private information. Management personnel are forbidden to disclose this information without the written consent of the employee, except as provided by law. With the written consent of the employee, appropriate other Agency personnel may be informed. Anyone who has access to such confidential information shall keep it confidential.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 20: HIV/AIDS WORKPLACE GUIDELINES

Employees are not to divulge any HIV/AIDS related information concerning any applicant for employment or client of the Agency. Violation of this policy may result in disciplinary action up to and including termination.

20.3 EDUCATION AND TRAINING

During the New Hire Orientation, new employees shall receive a copy of the Agency's workplace guidelines and an educational pamphlet published by the Texas Department of State Health Services.

All employees shall receive annual training and education about HIV/AIDS and its implications in the workplace. This shall include the current medical information about HIV/AIDS transmission and methods of prevention, confidentiality and related laws, and nondiscrimination.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 21: AMERICANS WITH DISABILITIES ACT (ADA)

21.0 PURPOSE

To provide a work environment and culture wherein no individual with a disability shall be discriminated against in employment or the provision of Agency services. Modifications shall be made to established policies, practices, and procedures to comply with the ADA.

Facilities and equipment that are required to be readily accessible to and usable by persons with disabilities shall be maintained in working condition.

Each program shall be conducted so that it is readily accessible to and usable by individuals with disabilities.

Steps shall be taken to ensure that communications with employees, applicants for employment, clients, and visitors with disabilities are as effective as communications with non-disabled individuals.

Auxiliary aids and services shall be furnished when necessary to afford an individual with a disability an equal opportunity to participate in and enjoy the benefits of an Agency service or program.

In determining the type of auxiliary aid or service to be provided, the request of the individual with the disability shall be honored if practicable.

21.1 DEFINITIONS:

A disability is defined by the ADA as:

- Any individual having a known physical or mental impairment that substantially limits at least one major life activity of the individual;
- Having a record of such an impairment; and
- Being regarded as having such an impairment.

A qualified individual with a disability who satisfies the requisite skill, experience, education and other job-related requirements of the employment position such individual holds or desires, and who, with or without reasonable accommodation, can perform the essential functions of such position, with or without reasonable accommodation.

21.2 EMPLOYMENT

The Agency shall not discriminate against any qualified employee or job applicant with respect to any terms, privileges, or conditions of employment because of that person's disability. The Agency shall also make reasonable accommodations wherever necessary for any employee or applicant with a disability, provided that the individual is otherwise

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 21: AMERICANS WITH DISABILITIES ACT (ADA)

qualified to satisfactorily perform the duties and assignments required of the job and provided that any accommodations do not create an undue hardship to the Agency. All job postings will include a statement that all reasonable workplace accommodations are requested by calling the ADA Coordinator. The ADA Coordinator will promptly respond to all such requests.

The Agency's policy of nondiscrimination applies to all employees and employment practices including, but not limited to, the following:

- Hiring;
- Reclassification;
- Promotion;
- Demotion;
- Transfer;
- Leave (all types);
- Recruitment or recruitment advertising;
- Layoff or termination;
- Job assignment;
- Compensation of any kind;
- Selection for training;
- Educational programs;
- Fringe benefits (including, but not limited to, medical insurance);
- Agency-sponsored recreational and social activities; and
- Disciplinary actions.

The HRD shall review all human resources procedures to determine whether job applicants and employees with disabilities are given nondiscriminatory consideration when job qualifications are assessed. All employment and advancement decisions shall be made on the basis of technical ability and/or professional experience for the particular job. In no event shall standards, criteria, or methods for such decisions have the effect of discrimination on the basis of disability. Actions taken to discourage discriminatory personnel practices include the following:

- Analyzing job descriptions to determine those tasks that are essential.
- Determining whether employment application forms contain questions regarding disabilities.
- Assessing the business necessity of job requirements, employment tests, or other criteria that may disqualify otherwise qualified individuals with disabilities.
- Determining whether physical barriers preclude access for the mobility-impaired.
- Evaluating the total selection process, including training and promotion, to determine whether discrimination against an otherwise qualified individual with a disability may occur or has occurred.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 21: AMERICANS WITH DISABILITIES ACT (ADA)

- Informing all personnel involved in employment practices about their obligations under the ADA.
- Requiring no medical examinations.
- Assisting disabled job applicants in completing forms.
- Making reasonable accommodations to qualified applicants or employees with disabilities, except when such accommodations will create undue hardship for the Agency.
- Maintaining, when possible, the confidentiality of the need to make a particular accommodation for an employee with a disability.
- Determining whether contractual agreements with employment or referral agencies, providers of fringe benefits, and providers of training or apprenticeship programs and similar organizations are nondiscriminatory.
- Providing recreational and social opportunities for employees with disabilities equal to the opportunities, if any, provided to non-disabled employees.
- Providing persons with disabilities an equitable opportunity to use parking facilities provided to other employees.
- Determining eligibility for vacations, sick leave, and leaves of absence without regard to disability.
- Maintaining the administration of Agency-sponsored programs, such as advanced education, management training, or business conferences, without discrimination on the basis of disability.
- Counseling applicants and employees with disabilities on the full range of career opportunities within the Agency, without regard to disability.

21.3 ADMINISTRATION AND IMPLEMENTATION

The Human Resources Manager is directly responsible for the ADA Compliance Program and is specifically responsible for the following functions:

- Developing policy statements, guidelines, and internal and external communications about the requirements of the ADA and the Agency's Compliance Program.
- Meeting with managers, supervisors, and employees to discuss any problems or concerns that may arise in accommodating individuals with disabilities.
- Keeping informed of the need for continuation or discontinuation of the workplace accommodation as reported by the employee with the disability.
- Determining the need for remedial action and recommending policies to correct any deficiencies in the program.
- Serving as liaison between the Agency and persons with disabilities, organizations representing individuals with disabilities, and agencies enforcing the ADA.
- All managers and supervisors are responsible for administering and complying with this policy with respect to the employees under their supervision.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 21: AMERICANS WITH DISABILITIES ACT (ADA)

21.4 DISSEMINATION OF POLICY

The Agency shall make every effort to disseminate this policy to all interested parties. Dissemination of this policy shall be accomplished by methods including, but not limited to, the following:

- Reproducing the same in this Manual.
- Posting the same on all Agency bulletin boards.
- Communicating with all employees through written literature and oral presentations.
- Including the same within the employee orientation program.
- Making the same available for inspection during normal business hours in the Human Resources Department.

21.5 CONFIDENTIALITY

Employees, job applicants, and visitors are assured that all information regarding a disability will be kept completely confidential, except that:

- Relevant supervisors and managers will be informed about restrictions on the work or duties of disabled employees and any accommodations that must be made;
- If the disability may require emergency treatment, first aid and safety personnel shall be so informed; and
- Government officials investigating compliance with applicable laws shall be informed.

All employees who acquire knowledge of disabilities are advised that they are to keep the information confidential.

21.6 ADA GRIEVANCE PROCEDURES

An employee who believes that he or she has been discriminated against on the basis of disability should immediately follow the guidelines set forth in Section 8: Employee Grievance Policy.

21.7 REASONABLE ACCOMMODATIONS, EMPLOYMENT TESTS AND WRITTEN JOB DESCRIPTIONS

Reasonable Accommodations

An employee requiring an accommodation shall notify his/her immediate supervisor in writing of the nature of the disability and the requested accommodation. The employee shall submit to the team leader and the HRD a written request which shall include a medical statement. The medical statement shall contain a diagnosis, prognosis, and evaluation as to the effect that the impairment will have on the employee's ability to perform the essential duties associated with the employee's position. The statement shall also include what major life activity is substantially limited as a result of the disability.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 21: AMERICANS WITH DISABILITIES ACT (ADA)

The process of reasonable accommodation, including when and how a request for accommodation is made, the accommodations considered, an analysis of the reasonableness of the costs of a proposed accommodation, the reasonableness of the administrative burden imposed by a proposed accommodation, and the reasons that a particular accommodation is chosen or rejected or no accommodation is implemented, shall be documented. It is not necessary to provide a reasonable accommodation if doing so would cause an undue hardship to the Agency. An “undue hardship”: exists where the particular accommodation considered would cause significant difficulty or expense to the Agency in light of the following factors:

- The nature and cost of the accommodation.
- The overall financial resources of the Agency.
- The impact of the accommodation upon the operation of the relevant division/section, including the impact on the ability of other employees to perform their duties and the impact on the division/section’s ability to conduct business and provide services to clients.

When a qualified employee requests an accommodation, the immediate supervisor shall take the following steps:

1. Consult with the Human Resources Manager to review essential functions of the particular job.
2. Confer with the disabled employee and ascertain the job-related limitations and how a reasonable accommodation would lessen those limitations.
3. Identify reasonable accommodations and assess the cost and effectiveness of each.
4. Ask the individual his or her preference for a reasonable accommodation.
5. If the only reasonable accommodation would create an undue hardship due to cost, determine whether financial assistance is available.
6. If financial assistance is not available and there are no other available reasonable accommodations, offer the individual the opportunity to pay for that portion of the accommodation that would create an undue hardship.
7. Prepare a written report for review by the section/division director documenting the essential functions of the position, type of accommodation requested, how requests will or will not be accommodated, and the reasons substantiating the decision within a reasonable period from the date of receipt of the requested accommodation and medical statement.

If a person rejects the reasonable accommodations and, as a result, cannot perform the essential functions of his/her job, that person may be considered unqualified for the job.

Final Authority on Reasonable Accommodations Decision

Division/section directors will inform the employee requesting an accommodation of any decision within a reasonable period from the date of receipt of the immediate supervisor’s

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 21: AMERICANS WITH DISABILITIES ACT (ADA)

report and recommendation for providing an accommodation. In the event an accommodation cannot be provided, the section/division director will document such findings and forward, within a reasonable period from the date of receipt, to the Secretary of State or the Deputy Secretary of State, who is the final authority on determining whether an accommodation would create an undue hardship to the Agency.

Section/division directors shall be required to present to the Secretary of State or Deputy Secretary of State information demonstrating that the implemented accommodation would cause an undue hardship.

The Secretary of State or the Deputy Secretary of State shall make a final determination within a reasonable period from the date of receipt of the report from the section/division director. The section/division director will inform the immediate supervisor and the employee of the final decision immediately upon receipt.

21.8 EMPLOYMENT TESTS

All employment tests administered by the Agency must:

- Actually measure what they purport to measure;
- Measure only job-related skills; and
- Be given in a non-discriminatory fashion.

21.9 WRITTEN JOB DESCRIPTIONS

Written job descriptions are to be prepared for every job before advertising to fill a position. In the case of a discrimination claim, written job descriptions shall be considered as evidence of the essential functions of a job.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 22: RETURN TO WORK PROGRAM

22.0 POLICY STATEMENT

The Agency seeks to provide a Return to Work Program as a means to return employees to meaningful, productive employment following injury or illness. To provide the highest level of quality service to the citizens of Texas, it is necessary for every employee of the Agency to be available and ready for work and capable of performing the duties and discharging the responsibilities for which he/she was hired.

The Return to Work Program provides opportunities for any employee who sustains or experiences an injury during the course and scope of employment, a “disability” as defined by the Americans with Disabilities Act (ADA) as amended, and/or a “serious health condition” as defined by the Family Medical Leave Act (FMLA) to return to “full duty” status as defined in Section 22.9 below. If the employee is not physically capable of returning to “full duty”, the Return to Work Program provides opportunities (when available) for the employee to perform a temporary assignment in which the employee’s regular position is modified to accommodate the employee’s physical limitations and/or restrictions, or to assume an alternative position.

The Return to Work Program shall not be construed as recognition by the Agency, its management, or its employees that any employee who participates in the program has a “disability” as defined by the ADA. If an employee sustains an injury or illness that results in a disability under the ADA, it is the employee’s responsibility to inform his or her supervisor, or another person in a management position, that a disability under the ADA exists and that a reasonable accommodation is necessary for the employee to perform the essential functions of his or her job.

Specific procedures shall be provided to advise all employees of the Return to Work Program. All employees of the Agency are expected to support and fully comply with this policy and the procedures provided to implement it.

22.1 ELIGIBILITY

An employee is considered eligible to participate in the Return to Work Program if he or she has sustained either:

- a compensable injury under the Texas Workers’ Compensation Act that results in lost time away from work;
- a serious health condition as defined by the FMLA; or
- a disability as defined by the ADA.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 22: RETURN TO WORK PROGRAM

22.2 NOTIFICATION OF INJURY, DISABILITY, OR SERIOUS HEALTH CONDITION

Employee Notification to Supervisor

An employee who sustains a compensable injury, disability, or serious health condition must notify the team leader, or a person in a higher management position, that such a condition exists. This notification shall occur at the earliest possible time after the occurrence of or knowledge of the condition.

Note to employees qualifying for FMLA-designated leave: The time period for notifying the Agency of the need to take FMLA-designated leave is set by statute.

Employees seeking to use FMLA-designated leave are required to provide thirty (30) days advance written notice of the need to take such leave, and of its anticipated timing and duration, when such need is foreseeable and such notice is practicable.

If the need to take FMLA-designated leave is not foreseeable, the employee should notify the Agency of the need to take such leave, and of its anticipated timing and duration, as soon as practicable under the facts and circumstances of the particular case. The Agency expects at least verbal notification within two (2) business days of the time the need for FMLA-designated leave becomes known to the employee if thirty (30) day advance written notice is not possible.

If the employee's injury or condition qualifies for protection under the ADA, the Agency shall provide a reasonable accommodation where possible, but the obligation to do so exists only for disabilities known to the Agency; it is therefore the employee's responsibility to notify the HRD that a disability under the ADA exists.

Response to Notification

Upon notification from the employee that he or she has a compensable injury, disability, or serious health condition, the Return to Work Coordinator shall provide the following information to the employee:

- A copy of Return to Work Program Policy and procedures and all appropriate forms as required. (Additional forms may be obtained from the Return to Work Coordinator or the Human Resources Department.)
- A copy of Agency's FMLA policy and procedures.
- A list of the essential and non-essential functions of the employee's job from the employee's team leader.
- A copy of the Workers' Compensation brochure, which describes workers' compensation benefits, including the payment of medical expenses and income payments.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 22: RETURN TO WORK PROGRAM

22.3 CERTIFICATION OF HEALTHCARE PROVIDER

Employees who must miss work for four (4) consecutive days or more due to a compensable injury, disability, and/or serious health condition must be certified or authorized by a healthcare provider to be off duty.

It is the employee's responsibility to ensure that the Healthcare Provider's Statement (see Appendix A) is completed and returned to the HRD in a timely manner (see below).

Foreseeable Leave

If the leave is foreseeable, the Healthcare Provider's Statement shall be provided to the HRD a minimum of three (3) business days prior to the time when leave will commence.

Note to employees taking foreseeable FMLA-designated leave: If the leave is foreseeable and at least thirty (30) days advance written notice has been given, the employee should provide the medical certification before the leave begins. When this is not possible, the employee must provide the medical certification by the date noted on the Employer Response to Employee Request for FMLA Leave Form.

Unforeseeable Leave

If the leave is not foreseeable, the certification form shall be provided to the HRD within three (3) business days after the initial visit to the health care provider.

Note to employees taking unforeseeable FMLA-designated leave: If leave is not foreseeable, the employee must provide the medical certification by the date noted on the Employer Response to Employee Request for FMLA Leave Form, or as soon thereafter as practicable under the particular facts and circumstances.

If the employee's injury or condition qualifies for protection under the ADA, the content of the Healthcare Providers Statement shall be limited to the opinion of the healthcare provider as to whether the employee can perform the essential functions of the job with or without a reasonable accommodation, and whether the employee would pose a significant harm that could not be reduced to an acceptable level with a reasonable accommodation.

22.4 STATUS REPORTS DURING LEAVE

The Agency will require a Return to Work Status (see Appendix A) every thirty (30) calendar days during the leave period regarding the employee's status and intent to return to work.

Note to employees on FMLA-designated leave: While Return to Work Status will be required of any employee participating in the Return to Work Program, employees on FMLA-designated leave may additionally be required to provide medical re-certification

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 22: RETURN TO WORK PROGRAM

of their FMLA-qualifying condition (Healthcare Provider's Statement), in accordance with the Agency's FMLA policy.

If the employee's injury or condition qualifies for protection under the ADA, the content of the Return to Work Status shall be limited to the opinion of the health care provider as to whether the employee could perform the essential functions of the job with or without a reasonable accommodation, and whether the employee would pose a significant harm that could not be reduced to an acceptable level with a reasonable accommodation.

22.5 RETURN TO WORK

When employees are authorized by a healthcare provider to return to work, the Return to Work Program provides opportunities for employees to return to work either at "full duty," or in a temporary or alternative assignment capacity where available if the employee is not physically capable of returning to work at "full duty".

"Full Duty"

An employee will be eligible to return to work at "full duty" when he/she are authorized by a healthcare provider (via Return to Work Status) to perform all essential and non-essential functions of his/her regular job.

Temporary Assignment Position

An employee will be eligible to return to work in a temporary assignment capacity where available when he/she is authorized by a healthcare provider (via Return to Work Status) to perform less than all essential and non-essential functions of the employee's regular job. A temporary assignment position may involve either a modified duty assignment or an alternative duty assignment.

"Modified Duty" Temporary Assignment

In a "modified duty" temporary assignment, an employee performs all the essential functions, but only a portion of the non-essential functions and tasks of the regular position for which the employee is employed. Modified duty allows employees to return to their regular jobs and perform those duties and tasks that are within their capabilities, given the restrictions imposed by the treating health care provider. Modified duty is a temporary arrangement until the injured employee can resume working at "full duty".

Note to employees with a disability under the ADA: A modified duty position may become a permanent arrangement as a reasonable accommodation, if such an accommodation does not create an undue hardship on the Agency.

"Alternative Duty" Temporary Assignment

In an "alternative duty" temporary assignment, an employee performs the essential functions of a job or position other than the position for which the employee is employed. Alternative duty allows the employee to temporarily perform other duties and tasks that

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 22: RETURN TO WORK PROGRAM

are within the capabilities of the employee, given the restrictions imposed by the treating health care provider. Such alternative duty may be physically located in the same facility or in some other facility. Alternative duty is a temporary arrangement until the injured employee can resume performing the full activities of his/her regular job.

Note to employees with a disability under the ADA: An alternative duty position may become a permanent arrangement as a reasonable accommodation, if such an accommodation does not create an undue hardship on the Agency.

Offer of Temporary Assignment Position

When an employee provides authorization from a healthcare provider (via Return to Work Status) to return to work at less than “full duty,” the Agency may offer a temporary assignment position, when available, to the employee. All temporary assignment positions shall be documented in a “bona fide offer of employment” letter to the employee.

The bona fide offer of employment letter shall include the following information:

- The state job classification title, a specific list of essential and non-essential job functions, and the maximum physical requirements of the temporary assignment position;
- The monthly salary rate for the position;
- The job location;
- A statement that the Agency is aware of and will accommodate any physical limitations under which the treating healthcare provider has authorized the employee to return to work;
- The expected duration of the temporary assignment;
- The consequences of not accepting a temporary assignment; and
- The person to contact if the employee has questions regarding the temporary assignment, job modifications, or the FMLA or ADA.

Section directors and manager/team leaders shall be responsible for identifying any temporary assignment positions on a case-by-case basis, taking into account the business necessity of filling the employee’s position, the employee’s entitlement to FMLA-designated leave, if any, and the availability of temporary assignments. Temporary assignments are not intended to displace other employees, nor are they intended to consist of menial tasks or simply “busy work.” The temporary assignment should consist of duties and tasks that constitute productive work for the Agency.

An employee may decline the offer of a temporary assignment position. However, an employee who declines an offer of temporary assignment position may be subject to any appropriate administrative penalties or disciplinary procedures. Additionally, the Texas Workers’ Compensation Act allows income benefits to be reduced when an employee

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 22: RETURN TO WORK PROGRAM

with a compensable injury refuses a “bona fide offer of employment” for a temporary assignment.

Note to employees on FMLA-designated leave: The FMLA provides that an employer may not require an employee who is on FMLA-designated leave to return to work during such leave, even if the health care provider treating the employee certifies that the employee is able to return to a temporary assignment position.

Such employee may thus decline the Agency’s offer of a temporary assignment position and remain on FMLA-designated leave for the remainder of his or her FMLA entitlement period without being subject to any administrative penalties or disciplinary procedures.. However, income benefits being received under the Texas Worker’s Compensation Act may be reduced regardless of FMLA-designated leave status.

Length of Temporary Assignment

The length of a temporary assignment shall be based on business necessity, but generally shall last no longer than thirty (30) calendar days. However, more serious injuries or illnesses may require a longer assignment period. Each case shall be handled individually, and each employee shall be informed at the outset of the duration of the temporary assignment position.

Expiration of Temporary Assignment Period

Employees must submit a Return to Work Status to the HRD at the end of the temporary assignment period. If the employee is unable to return to work at “full duty” by the end of the temporary assignment period and/or by the end of the employee’s FMLA-designated leave entitlement period, if applicable, then the employee’s continued employment with the Agency shall be considered based upon business necessity and whether any reasonable accommodation is required under the ADA.

Early Termination of Temporary Assignment

A temporary assignment position shall be terminated prior to the end of the assignment period when any one of the following circumstances occurs:

- the employee is authorized to return to work at full duty, with or without reasonable accommodation, by the treating health care provider;
- the employee finds other employment outside of the Agency; or
- the employee is dismissed from employment by the Agency.

22.6 USE OF PAID LEAVE

The Agency requires employees participating in the Return to Work Program to substitute paid leave for unpaid leave.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 22: RETURN TO WORK PROGRAM

Note to employees with a compensable injury under the Texas Workers' Compensation Act: An employee with a compensable injury under the Texas Workers' Compensation Act is not required to use all accrued annual or sick leave while participating in the Return to Work Program. The employee may elect to use, but may not be required to use, accrued paid sick leave before receiving workers' compensation temporary income benefits. However, if the employee elects to use paid sick leave, all such accrued leave must be exhausted before the employee shall be entitled to workers' compensation temporary income benefits.

22.7 RESPONSIBILITIES OF AGENCY SUPERVISORS

Return to Work Coordinator (RWC)

The RWC shall be responsible for coordinating all activities associated with the Return to Work Program, unless specific duties are otherwise assigned to another employee.

The RWC shall develop, maintain, and provide training through new employee orientation meetings and refresher training courses for current employees.

The RWC shall be responsible for maintaining regular communications with employees participating in the Return to Work Program to ensure that all questions of the employee have been answered, to encourage the employee during recuperation from the injury/illness, to encourage return to work at the earliest possible date, and to offer assistance to the employee. Any communication with the employee shall be documented. In the event that the RWC becomes aware of any circumstances that alter the employee's status as documented in the most current Return to Work Status he or she shall notify the manager/team leader of such circumstances.

The RWC shall review all Healthcare Provider Statements.

Manager/Team leader

The manager/team leader shall identify and document the essential and non-essential functions of all job positions for which he or she is responsible. The physical requirements of the position should be included in all position descriptions as either "essential" or "non-essential" functions.

Any communication with the employee shall be documented. In the event that the manager/team leader becomes aware of any special circumstances that alter the employee's status as documented in the most current Return to Work Status, he or she shall notify the RWC of such circumstances.

22.8 PROHIBITED ACTIONS

The Return to Work Program shall not be applied to any situation or circumstance in a manner that discriminates on the basis of race, color, sex, national origin, religion, or

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 22: RETURN TO WORK PROGRAM

disability. It is a violation of the Return to Work Program and state or federal law for any employee, supervisor, or manager of this Agency to do any of the following:

1. Discharge or in any other manner discriminate against an employee of the Agency because the employee:
 - Files a workers' compensation claim in good faith;
 - Hires a lawyer to represent the employee in a workers' compensation claim;
 - Institutes or causes to be instituted in good faith a proceeding under the Texas Workers' Compensation Act; or
 - Testifies or is about to testify in a proceeding under the Texas Workers' Compensation Act.
2. Discharge or in any other manner discriminate against an employee of the Agency because the employee:
 - Opposes any practice made unlawful by the FMLA or ADA;
 - Has filed any charge, or has instituted or caused to be instituted any proceeding under or related to the FMLA or ADA;
 - Has given, or is about to give, any information in connection with any inquiry or proceeding relating to any right provided under the FMLA or ADA; or
 - Has testified, or is about to testify, in any inquiry or proceeding relating to any right provided under the FMLA or ADA.
3. Interfere with, restrain, or deny the exercise of or the attempt to exercise, any right provided by the FMLA.
4. Discriminate on the basis of disability against any employee of the Agency who is a qualified individual with a disability under the ADA with regard to:
 - Job assignments, job classifications, organizational structures, position descriptions, lines of progression, and seniority lists;
 - Leaves of absence, sick leave, or any other leave;
 - Upgrade, promotion, award of tenure, demotion, transfer, layoff, termination, right of return from layoff, and re-hire;
 - Rates of pay or any other form of compensation, changes in compensation, and fringe benefits available;
 - Selection and financial support for training; or
 - Social and recreational activities.
5. Limit, segregate, or classify a job applicant or employee in a way that adversely affects his or her employment opportunities or status on the basis of a disability under the ADA.
6. Require a medical examination of an employee who is "disabled," as defined under the ADA, unless the medical examination is job-related and consistent with business necessity.
7. Make inquiries as to whether an employee is an individual with a disability or as to the nature or severity of such disability, unless such inquiry is job-related and consistent with business necessity.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 22: RETURN TO WORK PROGRAM

22.9 DEFINITIONS

Compensable Injury: A “compensable injury” is an injury that arises out of and in the course and scope of employment for which compensation is payable under the Texas Workers’ Compensation Act. “Injury” means damage or harm to the physical structure of the body and any disease or infection naturally resulting from such damage or harm. “Injury” also includes an occupational disease.

Disability: A “disability” is a physical or mental impairment that substantially limits one or more of the major life activities of an individual. “Major life activities” include functions such as caring for oneself, performing manual tasks, walking, seeing, hearing, speaking, breathing, learning, and working.

Leave under the Family and Medical Leave Act (“FMLA”): The FMLA provides for a federal leave entitlement of up to twelve (12) weeks under certain conditions, including when an eligible employee is unable to work because of his or her serious health condition. See Section 11, Family and Medical Leave Act (FMLA).

Full duty: Working at “full duty” entails performing all essential and non-essential functions of the employee’s regular job.

Lost Time: “Lost time” is that which is spent away from work at the direction of the treating health care provider as a result of a compensable injury sustained in the course and scope of employment. The term does not include time worked in a temporary assignment position.

Serious Health Condition: A serious health condition is an illness, injury, impairment, or physical or mental condition that involves:

- Inpatient care in a hospital, hospice, or residential medical care facility, including any period of incapacity; or
- Continuing treatment by a health care provider, including a period of incapacity.

Temporary Assignment: Performance of a temporary job assignment is intended to return an injured employee to work at less than his or her full duties when a compensable injury, disability, or serious health condition prevents the employee from working at full duty.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

**SECTION 23: SUBSTANCE ABUSE (DRUG-FREE AND ALCOHOL-FREE
WORKPLACE)**

23.0 PURPOSE AND GOAL

The Agency is subject to the Drug-Free Workplace Act of 1988 and is committed to protecting the safety, health, and “well-being” of all employees and other individuals in our workplace and to facilitate educational and treatment opportunities for all employees. We recognize that substance abuse poses a significant threat to agency goals. We have established a substance abuse-free workplace program that balances our respect for individuals with the need to maintain an environment free of substance abuse. We encourage employees to voluntarily seek help with substance abuse problems.

Nothing in the policy is intended to nullify the doctrine of “at-will” employment or to create an employment contract of any kind with any person.

23.1 COVERED WORKERS

Any individual who conducts business for the Agency, is applying for a position or is conducting business on the Agency’s property is covered by our substance abuse workplace policy. Our policy includes, but is not limited to, employees, contractors, volunteers, interns, and applicants.

23.2 APPLICABILITY

Our substance abuse workplace policy is intended to apply whenever anyone is representing or conducting business for the Agency. Therefore, this policy applies during all working hours, whenever conducting business or representing the Agency, while on or off Agency property, and at Agency-sponsored events, wherever they may be. This policy also applies to any activity affecting the employee’s suitability for continued employment, e.g., harming the reputation of the Agency, adversely affecting the employee’s job performance, or endangering the employee or other employees’ safety.

23.3 DEFINITIONS

- State Premises - All state property including vehicles, parking lots, and lockers.
- State Property - All owned and leased property used by state employees such as vehicles, lockers, desks, facilities, and rental vehicles.
- A “Controlled Substance” for the purpose of this policy means a substance listed on schedules I through V of Section 202 of the Controlled Substances Act (21 U.S.C. § 812), including, but not limited to, marijuana, heroin, cocaine, methamphetamine, or anabolic steroid.
- Drug - Any chemical substance that produces a physical, mental, emotional, or behavioral change in the user.
- Drug Paraphernalia - Equipment, a product, or material that is used or intended for use in concealing an illegal drug or for use in injecting, ingesting, inhaling, or otherwise introducing into the human body an illegal drug or controlled substance.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

**SECTION 23: SUBSTANCE ABUSE (DRUG-FREE AND ALCOHOL-FREE
WORKPLACE)**

- **Illegal Drug** - Any drug or derivative thereof of which the use, possession, sale, transfer, attempted sale or transfer, manufacture, or storage is illegal or regulated under any federal, state, or local law or regulation; and any other drug, including, but not limited to, a prescription drug used for any reason other than a legitimate medical reason by the individual for whom it is prescribed and in the amount and manner for which it is prescribed, and inhalants used illegally. All forms of marijuana or cannabis are included.
- **“Under The Influence”** for the purpose of this policy means the state of not having the ordinary use of mental or physical faculties resulting from the introduction into the body of an intoxicating substance or a controlled substance.
- An **“Intoxicating Substance”** for the purpose of this policy means a legal substance whose misuse or overuse may lead an employee to lose his/her ordinary mental or physical faculties. These substances include, but are not limited to, alcohol, prescription drugs, over-the-counter medications, herbs, or inhalants.

23.4 PROHIBITED BEHAVIOR

It is a violation of the substance abuse policy to manufacture, distribute, sell, dispense, possess, or use controlled substances, illegal drugs and drug paraphernalia, and alcoholic beverages; and to abuse inhalants or prescription drugs.

It is a violation of this policy to consume alcohol, be intoxicated, be under the influence of illegal drugs, intentionally misuse a product that impairs work performance, or take non-prescribed medication (excluding over the counter medication) while on the job.

Intoxication is defined as:

1. Having an alcohol concentration .08 or more; or
2. Not having the normal use of mental or physical faculties resulting from the voluntary introduction into the body of:
 - An alcoholic beverage, as defined by Section 1.04, Alcoholic Beverage Code;
 - A controlled substance or controlled substance analogue, as defined by Section 481.002, Health and Safety Code;
 - A dangerous drug, as defined by Section 483.001, Health and Safety Code;
 - A drug;
 - A combination of two or more of those substances;
 - An abusable glue or aerosol paint, as defined by Section 485.001, Health and Safety Code; or
 - Any similar substance, the use of which is regulated under state law.

Intoxication does not include the loss of normal use of mental or physical faculties resulting from the introduction into the body of a substance:

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

**SECTION 23: SUBSTANCE ABUSE (DRUG-FREE AND ALCOHOL-FREE
WORKPLACE)**

1. Taken under and in accordance with a prescription written for the employee by the employee's doctor; or
2. Listed above by inhalation or absorption incidental to the employee's work.

The General Appropriations Act prohibits the payment of salaries to employees who consume alcoholic beverages while on duty.

An employee who reasonably suspects a fellow employee of violating this policy may so advise his/her manager/team leader. Such manager/team leader shall then consult with the section/division director of the applicable section/division who will then undertake whatever investigation, if any, and initiate such disciplinary process, if any is deemed warranted. The anonymity of the complainant shall be preserved. The Human Resources Manager shall be available to provide direction in complying with disciplinary procedures and/or to answer related questions.

Employees may not engage in activities that adversely affects the employees' suitability for employment. Compliance with this policy is a strict condition of continued employment for all employees.

23.5 NOTIFICATION OF CONVICTIONS

Any employee who is convicted of a criminal drug violation in the workplace must notify his/her section/division director in writing within five (5) calendar days of the conviction. The agency, consistent with requirements of the Rehabilitation Act of 1973 and the Americans with Disabilities Act, will take appropriate disciplinary action within ten (10) days of receipt of the written notification. Federal contracting agencies will be notified when appropriate.

23.6 SEARCHES

Entering the Agency's property constitutes consent to searches and inspections. If an employee is suspected of violating the substance abuse workplace policy, he or she may be asked to submit to a search or inspection at any time. Searches can be conducted of desks and work stations.

23.7 CONSEQUENCES

One of the goals of our substance abuse workplace program is to encourage employees to voluntarily seek help with substance abuse problems. If an employee violates the policy, he or she will be subject to progressive disciplinary action and may be required to enter rehabilitation. An employee required to enter rehabilitation who fails to successfully complete it and/or repeatedly violates the policy will be terminated from employment. Nothing in this policy prohibits the employee from being disciplined or discharged for other violations and/or performance problems.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

**SECTION 23: SUBSTANCE ABUSE (DRUG-FREE AND ALCOHOL-FREE
WORKPLACE)**

In the case of applicants, if he or she violates the substance abuse workplace policy, the offer of employment can be withdrawn. The applicant may reapply after six months.

23.8 RETURN-TO-WORK AGREEMENTS

Following a violation of the substance abuse policy, an employee may be offered an opportunity to participate in rehabilitation. In such cases, the employee must sign and abide by the terms set forth in a Return-to-Work Agreement as a condition of continued employment.

23.9 TREATMENT

The Agency recognizes that substance abuse and addiction are treatable illnesses. We also realize that early intervention and support improve the success of rehabilitation. To support our employees, our substance abuse workplace policy:

- Encourages employees to seek help if they are concerned that they or their family members may have a substance abuse problem.
- Allows the use of accrued paid leave while seeking treatment for substance abuse problems.
- Encourages employees to utilize the services of qualified professionals in the community to assess the seriousness of suspected substance abuse problems and identify appropriate sources of help.

The Agency does not have an Employee Assistance Program (EAP). Treatment for alcoholism and/or other drug use disorders may be covered by the employee's medical insurance plan. However, the ultimate financial responsibility for recommended treatment belongs to the employee.

Employees may contact any of the following organizations for treatment programs and other information regarding substance abuse.

- Texas Department of State Health Services Substance Abuse Services. 877-9-NO DRUG (877-966-3784). www.dshs.state.tx.us/sa
- Alliance Work Partners, 2525 Wallingwood Dr., Austin, TX 78746. 512-328-8519; 800-342-3822. www.alliancewp.com
- The American Council on Alcoholism helpline provides referrals to alcohol treatment programs nationwide and provides written materials. 1-800-527-5344. www.aca.usa.org. E-mail: info@aca-usa.org
- The National Council on Alcoholism and Drug Dependency provides written information on alcohol abuse and provides a referral service to treatment and counseling centers across the country. 1-800-NCA-CALL (1-800-622-2255). www.ncadd.org. E-mail: national@ncadd.org
- The National Institute on Drug Abuse hotline is a federally-funded service providing referrals to drug and alcohol programs including referrals for those who cannot pay for services. 1-800-662-HELP (1-800-662-4357). www.findtreatment.samhsa.gov

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

**SECTION 23: SUBSTANCE ABUSE (DRUG-FREE AND ALCOHOL-FREE
WORKPLACE)**

23.10 CONFIDENTIALITY

All information received by the Agency through the substance abuse workplace program is confidential communication. Access to this information is limited to those who have a legitimate need to know in compliance with relevant laws and management policies.

23.11 SHARED RESPONSIBILITY

A safe and productive workplace free of substance abuse is achieved through cooperation and shared responsibility. Both employees and management have important roles to play.

All employees are required to not report to work or be subject to duty while their ability to perform job duties is impaired due to on- or off-duty use of alcohol or other drugs.

In addition, employees are encouraged to:

- Be concerned about working in a safe environment.
- Support fellow workers in seeking help.
- Report dangerous behavior to their manager/team leader.

It is the manager's/team leader's responsibility to:

- Inform employees of the drug-free workplace policy.
- Observe employee performance.
- Investigate reports of dangerous practices.
- Document negative changes and problems in performance.
- Counsel employees as to expected performance improvement.
- Clearly state consequences of policy violations.

23.12 COMMUNICATION

Communicating our substance abuse workplace policy to both managers/team leaders and employees is critical to our success. To ensure all employees are aware of their role in supporting our substance abuse workplace program:

- All employees will receive a written copy of the policy and sign an acknowledgement of receipt of the policy.
- The policy will be reviewed in orientation sessions with new employees.
- The policy and assistance programs will be reviewed at safety meetings.
- All employees will receive an update of the policy annually.
- Posters and brochures will be available at all locations.
- Employee education about the dangers of substance abuse and the availability of help will be provided to all employees annually.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 24: SERVICE AWARDS

24.0 PURPOSE

The Agency shall purchase and present to employees service awards for longevity with the State of Texas. The Agency shall purchase awards not to exceed \$100.00 per employee.

24.1 OBJECTIVE

Recognize employees in a timely and consistent manner who have obtained five (5) or more years of service with the State of Texas.

24.2 POLICY

Employees who have been employed by the State of Texas for five (5) or more years will be presented an award on their 5th anniversary and on a 5-year increment basis thereafter.

Awards will be limited to the following:

5 th Anniversary	Framed Certificate of Recognition from the Secretary of State
10 th Anniversary	Framed Certificate of Recognition from the Secretary of State Pewter and Brass Dome Paper Weight w/ Texas State Seal
15 th Anniversary	Framed Certificate of Recognition from the Secretary of State Wooden Pen and Pencil Set in Wooden Case that displays the Texas State Seal
20 th Anniversary	Framed Certificate of Recognition from the Secretary of State Texas State Seal Glass Name Plate
25 th Anniversary	Framed Certificate of Recognition from the Secretary of State Glass State Seal Clock
30 th Anniversary	Framed Certificate of Recognition from the Secretary of State Employee Choice of Gift – Item chosen must be state related. NOT TO EXCEED A TOTAL OF \$100.00
Retirement	Framed Certificate of Recognition from the Governor of Texas Framed Certificate of Recognition from the Secretary of State Employee Choice of Gift – Item chosen must be state related. NOT TO EXCEED A TOTAL OF \$100.00

EXCEPTION TO POLICY: The employee’s division/section may sponsor an agency-wide event for an employee who is retiring from the State of Texas. The employee must

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 24: SERVICE AWARDS

be retiring in accordance with the rules and regulations of the Employees Retirement System. The employee will be eligible to receive an Agency gift as stated above and may receive other privately funded gifts. The employee's division/section will be responsible for all arrangements regarding the event. The Administrative Services Division will be responsible for acquiring the Agency gift upon notification from the division/section.

24.3 NOTIFICATION

The HRD will provide the Service Award Committee at the beginning of each quarter of the fiscal year (September, December, March, and June) a list of employees who will become eligible to receive a service award during the current quarter.

24.4 PRESENTATION OF AWARDS

Presentation of awards will be on the first Tuesday following the end of the quarter. An employee assembly will be conducted in the 4th Floor Atrium of the James Rudder Building where the Secretary of State and/or the Deputy Secretary of State will present the individual awards.

Division and section directors will also be given an opportunity to present a congratulatory message to their employees.

Individual divisions/sections that want to conduct additional activities may do so within the limits of their own divisions and invited guests.

24.5 SERVICE AWARD COMMITTEE

The Service Award Committee will be comprised of a representative from each division/section (Business Entity Filings, Government Filings, Uniform Commercial Code, Elections, Administrative Services, and Information Resources Technology). These individuals:

1. Schedule the Secretary of State and/or Deputy Secretary of State to be present at the ceremony.
2. Contact the HRD to reserve the 4th Floor Atrium upon confirmation from the Secretary of State or Deputy Secretary of State.
3. Confirm with the HRD the total number and types of awards to be presented during the quarterly service award ceremony.
4. Prepare an agenda for the ceremony (including notes for the Secretary of State or Deputy Secretary of State). (List of names, length of service, division, classification, etc.)
5. Order the Secretary of State certificates from the Executive Division, providing the name and length of service of each employee that will attain their service award eligibility date during the current quarter.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 24: SERVICE AWARDS

6. Prior to the ceremony, make arrangements to accompany and purchase gifts for the employees who have reached their 30th or above service award eligibility date. Each committee representative is responsible for the employee within their own division/section who will reach 30 or more years of service or retire from the State of Texas. The committee representative must contact the Purchasing Department for a purchase order to purchase an award.
7. Frame the certificates before the ceremony.
8. Arrange the podium and other furniture as needed in the atrium.
9. Conduct post-ceremonial cleanup.

24.6 PROCEDURE TO PURCHASE AN AWARD

The Administrative Services Division will order and purchase, at the beginning of the fiscal year, the number of awards anticipated to be distributed during the fiscal year. In addition, plaques will be ordered in advance to facilitate the mounting of certificates.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 25: SAFETY

25.0 INTRODUCTION

The Office of the Secretary of State regards employees as our most important asset, and their safety as our greatest responsibility.

The goal of this safety policy statement is to develop positive attitudes regarding accident prevention for all employees. Directors, managers, and team leaders are to be continuously cognizant of the safety of their employees and the general public. Directors, managers, and team leaders are charged with the responsibility of initiating necessary preventative measures to control hazards associated with functions under their control. It is essential that all directors, managers, and team leaders accept this responsibility for the safety of personnel coming into their areas of control and for the safety of personnel under their jurisdiction. Safety shall be incorporated as an integral part of all programs.

The responsibility for the administration of the accident prevention program is assigned to Greg Jones, who uses recognized safety standards to fulfill his responsibilities. This safety policy statement and the accident prevention program for the Office of the Secretary of State have the full support of this administration.

25.1 ASSIGNMENT OF DUTIES, RESPONSIBILITY, AUTHORITY, AND STAFFING

Safety Officer (SO): The SO is responsible for establishing and maintaining the Safety and Health Program. To accomplish this, the SO shall:

1. Prepare information on the Agency's Safety and Health Program (SHP) to be presented to all new employees.
2. Annually review and update the SHP and recommended program goals, as necessary.
3. Promote safety awareness through the distribution of educational materials such as posters, flyers, and brochures.
4. Ensure that safety and health issues are presented and discussed at appropriate staff meetings in conjunction with training on safety and health topics.
5. Coordinate with the State Office of Risk Management (SORM) and the Workers' Compensation Division (DWC) of Texas Department of Insurance on matters of mutual interest and concern.
6. Conduct and document a safety inspection of the Agency at least annually to detect and correct hazards.
7. Maintain a record of all on-the-job injuries or illnesses, and coordinate proper reporting with the Workers' Compensation Claims Coordinator (Claims Coordinator).
8. Develop safety and health related budget items on a timely basis.
9. Ensure that accidents are thoroughly investigated and appropriate corrective actions taken.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 25: SAFETY

10. To the extent practical and possible, consistent with Texas Facilities Commission (TFC) and other State rules concerning purchasing, ensure compliance with applicable safety standards in the purchase of Agency supplies and other property and services.

Managers and Team Leaders: Managers and Supervisors at all levels will provide leadership for the SHP and are responsible for minimizing on-the-job accidents by emphasizing safety and health to all employees. To do this, managers and team leaders shall:

1. Observe employees' work practices and take immediate action to reinforce safe behavior or correct unsafe conditions noted.
2. Include discussions and training on safety and health related issues and topics on a regular basis during staff meetings.
3. Report any accident, immediately after occurrence, to the Claims Coordinator and ensure that reporting procedures are implemented.
4. Take immediate action to report or to correct any noted safety hazard in the area of responsibility and control.
5. Support the Agency and SHP by word and deed.

Employees: Each employee is responsible for providing for his/her own safety to the maximum extent possible. To accomplish this, each employee shall:

1. Attend and participate in training and discussions concerning safety and health issues and concerns.
2. Report to a manager/team leader any safety hazard, that cannot be immediately corrected.
3. Report to work in a physical condition that will allow safe accomplishment of the job.
4. Immediately report any and all injury-producing accidents to a manager/team leader, including any "near-miss" incidents, which may or may not result in property damage.
5. Take whatever action is necessary to prevent accidents.
6. Seek training opportunities regarding safe-work practices and safe operating procedures.

25.2 Hazard Identification, Reporting, and Evaluation

In the event of an accident, whether it results in injury or not, the supervisor should be contacted immediately, as well as the Workers Compensations Claims Coordinator. The Claims Coordinator will complete the Employer's First Report of Injury or Illness (TWCC-1s). The injured employee will complete the Employee's Report of Injury (SORM-29) and the Authorization for Release of Information (SORM-16). Any witnesses to the accident will be required to complete a Witness Statement (SORM-74). When an injured employee is losing time from work, there are additional forms that must be submitted to SORM. In those cases the Claims Coordinator will assist the employee

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 25: SAFETY

in completing all of the necessary forms. The Claims Coordinator will notify the Safety and Health Office of each accident and a complete investigation will be conducted. Once the investigation is complete, a report will be submitted to management for review and a copy of the investigation report will be placed in the accident file.

25.3 AED DESCRIPTION

The AED is a self-testing, battery-operated automated external defibrillator (AED). After applying the AED’s electrodes (pads) to the patient’s bare chest, the AED automatically analyzes the patient’s electrocardiogram (ECG) and advises the operator to push the button and deliver a shock if needed. The AED uses one button and guides the operator through the rescue using a combination of voice prompts, audible alerts, and visible indicators.

Employee Responsibility

In the event an employee or customer suffers sudden cardiac arrest, you should call 911 immediately then call HR at 463-8000. HR will notify the first responder team and they will assist the employee or customer until an emergency medical crew arrives.

First Responders Responsibility

Employees who are cardiopulmonary resuscitation (CPR) certified and wish to be a First Responder will need to contact the Agency Safety Officer. First responders will be called to assist in the event an employee or customer is exhibiting symptoms of sudden cardiac arrest and is unresponsive and not breathing. First responders must remain CPR certified and will be trained on the use of the AED.

First Responder Team

The following employees are CPR certified and are AED First Responders.

Greg Jones	Administrative Services	475-2754
Evangeline Ramos	Administrative Services	463-5603
Mary Ann Conkel	Business Entity Filings	4-5557
ClarissaRodriquez	Business Entity Filings	4-1111
Reba Swonke	Business Entity Filings	475-0828
Sondra Hadley	UCC	475-2740
Ernest Fuentes	Elections	463-2835

Indications for Use

The AED is intended to be used by employees who have been trained in its operation. The user should be qualified by training in basic life support (CPR). The device is indicated for emergency treatment of employees and customers exhibiting symptoms of sudden cardiac arrest who are unresponsive and not breathing.

Safety Officer Responsibilities

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 25: SAFETY

Verify and document a check to ensure all AED equipment is available, clean, not outdated, and in good working condition every three months. Verify the status indicator light is green. If the status indicator light is red, do the following:

- Check the expiration date on the AED pads. Order new pads for the AED at least two months prior to the expiration date.
- Check the battery level. If the battery level is low, order a new one.
- Call customer service at 1-888-466-8686 if the AED is not in working status after you have performed all the checks.
- The AED will self-test every month and if maintenance is required, a beep will sound every thirty seconds until the lid is opened. After the AED has been used, prepare it for the next rescue. Connect a new pair of pads, close the lid, and verify the status indicator light is green. The Agency Safety Office will schedule CPR/AED training on a regular basis to ensure employees' certifications are current.

25.4 EMPLOYEE EDUCATION

Each new employee of the Agency will receive a safety orientation briefing by the Safety Officer. Because of the diversity of job tasks and work areas, the safety orientation will be general in nature. All new employees will receive the following safety related information during New Employee Orientation. New Employee Orientation will be conducted on a quarterly basis each fiscal year. Each item will be checked off and upon completion of the employee orientation is signed by the Safety Officer and employee.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 25: SAFETY

**Office of the Secretary of State
Employee Safety Orientation Form**

Employee Name: _____

Employment Date: _____

This form is to be completed by the Safety Officer for every new or transferred employee.

The following items have been reviewed on this date: _____

1. Employee's Safety Responsibilities _____
2. Emergency Response/First Aid Response _____
3. Agency Safety and Health Policy _____
4. Reporting Unsafe Working Conditions _____
5. Management Support for Working Safely _____
6. Accident Reporting Procedures _____
7. Review of Fire and Emergency Evacuation Plan _____
8. Workers' Compensation Programs/Benefits _____
9. Agency Drug Free Workplace Policy _____
10. Local Hazards _____

Safety Officer _____ Employee _____

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 25: SAFETY

1. **Employees' Safety Responsibilities** – Employees should be provided with an explanation of safety responsibilities and any pertinent safety rules. This will include the role and responsibilities of the Safety Officer, managers/supervisors, and individual employees.
2. **Emergency Response/First Aid Response** – Employees will be informed of the Agency's specific procedures for responding to a medical emergency.
3. **Agency Safety and Health Policy** – All new employees will be informed of the location on the Novell-delivered Application of the Agency's policy concerning employee safety and health.
4. **Reporting Unsafe Working Conditions** – Employees will be informed of their responsibility to report any hazard, hazardous condition, and known or suspected violations of any safety and health standard to their immediate supervisors. The procedure of when, where, and how to report unsafe working conditions will be explained.
5. **Management Support for Working Safely** – All new employees will be informed that they have management's support to always work safely. Employees will never undertake any job or operate any vehicle considered to be unsafe until the unsafe condition is corrected.
6. **Accident Reporting Procedures** – The Agency has specified procedures to guide employees in the steps that should be taken following an accident, incident, injury, or occupational disease. These procedures will be explained to each new employee at the time of New Employee Orientation.
7. **Review of Fire and Emergency Evacuation Plan** – All new employees will receive a thorough explanation of the Agency's fire extinguishers, fire alarm station, how to report a fire or other emergency, such as a bomb threat, and a copy of the Agency evacuation plan.
8. **Workers' Compensation Programs/Benefits** – All new employees will be informed of the workers' compensation benefits that are available if he/she incurs a compensable injury during the course and scope of employment.
9. **Agency Drug Free Workplace Policy** – The Agency's Drug and Alcohol Free Workplace Policy will also be explained to each new employee at the time of hire. Each employee will receive and sign a copy of the policy for his/her personnel file.
10. **Local Hazards** – Each new employee will be briefed on any known local hazards affecting personal safety and health. Examples include, but are not limited to, local traffic hazards, environmental hazards, potential for severe weather conditions, high crime areas, personal safety concerning parking, etc.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 25: SAFETY

25.5 SAFETY COMMITTEE

Greg Jones	Safety Committee Officer	475-2754
Michael Orta	Corporations	475-4285
Jill Ledbetter	Government Filings	475-9623
Helen Lupercio	Corporations	463-0864
Tinka Adkins	UCC	463-0607
Mary Ann Soto	Administrative Services	463-5598
Coby Simpson	Information Technology	463-2664
Ernest Fuentes	Elections	463-2835
Liz Harris	Executive	463-5702

25.6 FIRE AND EVACUATION PROCEDURES

Rudder Building

If an alarm sounds on a floor it will ring on that floor only. Within three (3) minutes all alarms in the building will sound and everyone must evacuate at that time.

When the alarm sounds on your floor, evacuate the building according to the Evacuation Plan located in each elevator lobby. After exiting the building, employees should cross Brazos Street and gather in parking lot 27, west of the Greer building. You are not required to evacuate if the alarm is not sounding on your floor, but if you feel this is necessary, please do so.

Rusk Building

If the fire alarm sounds on one floor in the Rusk Building then the fire alarm will automatically sound on the floor above and below the floor where the alarm originated. If Capitol Police does not cut off the alarm within ten (10) minutes, all of the alarms in the building will sound and everyone must evacuate at that time.

When the alarm sounds on your floor, evacuate the building according to the Evacuation Plan located in each elevator lobby. After exiting the Rusk building, employees should gather in front of the Fox 7 TV station. You are not required to evacuate if the alarm is not sounding on your floor, but if you feel this is necessary, please do so.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 25: SAFETY

Capitol Building

The Capitol Building has a Fire Marshall assigned to that building at all times. If a fire alarm is activated in the Capitol, the Fire Marshall will investigate, and if needed he/she will sound the fire alarm.

When the fire alarm sounds in the Capitol Building, all employees must evacuate using the east wing and gather in front of the Library and Archives building.

General Fire and Evacuation Procedures

Fire Extinguishers can be used, if needed. Instructions are on the label located on the extinguisher. If the fire is more than a trash can blaze, please do not attempt to put it out, pull the alarm trigger and call 911.

If you smell or see smoke, and feel there is a possible fire, call Capitol Police immediately and leave the area. Activate the alarm on your way out of the building. The alarm trigger system will sound the fire alarm and all employees will evacuate the building at that time.

Note: The building smoke detectors are very sensitive and will possibly sound the fire alarm when food is overcooked. Therefore, in order to avoid a false alarm, DO NOT leave such appliances as the microwave or toaster unattended when in use.

25.7 FIRE WARDENS

Revised 05/01/2012

Basement - Rudder Building

Greg Jones
Cedric Allen

First Floor - Rudder Building

Kika Garza
Michael Orta

Second Floor - Rudder Building

Jill Ledbetter Dana Blanton
Helen Lupercio

Third Floor - Rudder Building

Ron Parks
James Nino

Fourth Floor - Rudder Building

Jim Martin

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 25: SAFETY

Jeff Staton

Fifth Floor - Rudder Building

Fred Freedman

Earl Harrigan

Rusk Building

Ernest Fuentes

Terry Kays

Capitol Building

Elizabeth Harris

25.8 EMERGENCY PHONE NUMBERS

Capitol Complex Emergency Numbers

- Department of Public Safety Emergency Assistance , 463-3333
- DPS Assistance/Information, 463-3556

Other Emergency Numbers

- EMS 911
- Fire 911

25.9 OCCUPATIONAL SAFETY AND HEALTH

Keyboard Workstation Self-Evaluation Checklist

This self-evaluation checklist is to be used for preventive measures only. Where an injury or symptoms are already being experienced the Safety Officer or Workers' Compensation Claims Coordinator will need to be contacted for appropriate advice and, if necessary, conduct an ergonomic evaluation of your workstation. If you cannot modify or correct the identified deficiencies on your own, you should provide this checklist to your supervisor for assistance.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 25: SAFETY

**PRELIMINARY KEYBOARD WORKSTATION SELF-EVALUATION
CHECKLIST**

1. Keyboard and Mouse		OK
Keyboard height	Adjust keyboard height so arms and forearms are at right angles or slightly greater and forearms and hands form straight lines.	
Keyboard-to-user distance	Keyboard-to-user distance should allow user to relax shoulders with elbows hanging close to body.	
Keyboard slope	Position keyboard flat.	
Mouse-to-user distance	Mouse should be directly next to the keyboard.	
Mouse height	Adjust mouse so it is on the same level as the keyboard.	
2. Chair		
Seat height	Adjust seat height so feet are flat on the floor or footrest, knees are bent at right angles, and thighs are horizontal to floor.	
Seat back	Adjust seat back so it supports the lumbar curve of the low back.	
Seat pan tilt	Adjust seat pan tilt so hips and tops of thighs are at right angles or slightly greater.	
Armrest position	If possible, adjust armrests so that they are out of the way while typing, but may provide support during other activities (i.e. phone use, meetings, etc.).	
3. Monitor		
Monitor height	Adjust monitor height so top of screen is at or slightly lower than eye level.	
Screen-to-user distance	Viewing distance is approximately arms distance away (350 - 750 mm).	
Monitor alignment	Monitor and keyboard should be placed directly and symmetrically in front of user.	
Visual comfort of screen	Monitor should be positioned to avoid glare (perpendicular to window or strong light source).	
4. Work Environment and Work Surface		
Placement of frequently used items	Keep frequently used items (i.e. phone) close at hand.	
General task lighting	Ensure lighting is not direct or overly bright.	
5. Work Practices		
Frequency of pausebreaks	Get out of chair at least once per hour; do pausebreaks every 30-min of keyboarding.	
Keyboarding	Keep wrists straight, avoid supporting wrists on any surface	

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 25: SAFETY

posture	while typing.	
Sitting posture	Upright or slightly reclined posture, maintain slight hollow in lower back.	
Telephone posture	Avoid tilting head/neck to cradle the phone. Use hand to hold receiver or wear headset.	
Alternative tasks	Break up long periods of continuous computer use by performing other tasks.	

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 25: SAFETY

25.10 SAFETY CHECKLIST

Ergonomics

- Work can be performed without eyestrain or glare to the employees.
- Task does not require prolonged raising of the arms.
- Neck and shoulders are not stooped to view the task.
- There are no pressure points on any parts of the body (wrists, forearms, back, or thighs).
- Work can be done using the larger muscles of the body.
- Work can be done without twisting or overly bending the lower back.
- There are sufficient rest breaks, in addition to the regular rest breaks, to relieve stress from repetitive-motion tasks.
- All pieces of furniture are adjusted, positioned, and arranged to minimize strain on all parts of the body.

Aisles, Floors

- Aisle clearance is adequate for two-way traffic and for unobstructed access to all parts of the office and building.
- Office arrangement allows easy egress under emergency conditions.
- Floors are clear of pencils, bottles, electrical/phone cords, loose tiles, wastebaskets, briefcases, projections or other objects/protrusions on the floor that create a tripping hazard.
- Carpeting is in good condition and not badly worn or torn.

Office Furniture and Equipment

- Office furniture, equipment, and electrical appliances are arranged to obtain maximum safety and use of installed facilities, such as overhead lighting, wall outlets, telephones, and other services.
- Desks, file cabinets, etc., are arranged so that drawers do not open into aisles or walkways.
- Desk and file drawers are closed after use.
- Weight is distributed in file cabinets so that upper drawer contents do not create a top-heavy condition.
- Cabinets, bookcases, and shelves are secured to building surfaces to prevent their falling over.
- Faulty desks, chairs, or other office equipment are repaired or taken out of service.
- Sufficient lighting is provided in all working areas, including emergency lighting.
- Paper cutter blades are in the locked position when not in use.
- Knife blades have guards when not in use.
- Shelves are not overloaded.

Electrical Equipment

- Extension cords if used are in good condition – no splices or broken insulation.
- Cords and plugs are in good condition.
- Electrical cords are not run through openings in doors, walls, and ceilings or under carpets.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 25: SAFETY

- Multi-outlet strips are not plugged into other multi-outlet strips. Extension cords are not plugged into other extension cords.
- Wall outlet and junction box covers are in place.
- Limit extension cords to ten feet in length.
- Extension cords are to be used as a temporary remedy. The preferred choice over extension cords is to use multi-outlet strips. If multi-outlet strips are required, contact the Information Technology division.

Housekeeping

- Good housekeeping is maintained to minimize accidents.
- Ladders are provided for reaching materials on shelves and are kept in good repair.
- Paper and materials are stored properly.
- Combustibles are not stored under tables, desks, or shelves.
- Cleaning fluids are used only in small quantities and are stored in closed containers that are kept in well-ventilated areas. If flammable, they are not used near an open flame or a heating element.
- Excess paper, cartons, and trash are removed on a regular basis.

Emergency Preparedness

- Staff is familiar with emergency signals, procedures, exit routes, and emergency equipment (i.e., fire extinguisher, pull station) usage in the building.
- Emergency numbers are prominently posted.
- Fire doors are not blocked open.
- Exits are kept unlocked and not obstructed during normal business hours or special events.
- Exits are properly marked, and exit signs are illuminated.
- Drills are performed and critiqued.

Stairways, Ramps, Storage Areas

- Ramps have non-slip surfaces.
- Stair treads are in good condition.
- Stairways are clear and not used for storage.
- Stairways have handrails in good condition.
- No items are stored within 18 inches of sprinkler heads.

25.11 SAFE LIFTING TECHNIQUES

- **Size Up the Load** - Always assess the object before lifting it. Make sure the load is stable and balanced. Carefully and slowly put force against the object to determine its weight. If the load is too heavy, get help. Use lifting devices and equipment to assist in lifting/carrying a load.
- **Plan the Job** - Plan a route that is free of tripping and slipping hazards. Ensure that the planned route allows for easy travel. Know where the object will be unloaded and plan for rest stops if necessary. Think through the lift. Face the object to be lifted and, if possible, face the direction in which the object is to be carried. Do not twist the body.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 25: SAFETY

- **Establish a Base of Support** - Ensure firm footing. Keep the feet at least shoulder width apart. A staggered stance, with one foot slightly behind the other, often helps provide a firm base of support.
- **Bend the Knees** - Bend at the knees, not at the waist. Bend down as far as necessary using the legs and not the back.
- **Get a Good Grip** - Grip the load firmly, using the whole hand, not just the fingers. Use gloves, as needed, to prevent "pinched" grips or to protect the hands during the lift.
- **Keep the Load Close** - Keep the load close to the body. The closer it is to the spine, the less force it exerts on the back. Maintain the natural inward curve of the lower back. Keep the back upright. Whether lifting or putting down a load, do not add the weight of the body to the load. Grasp the object with the palms, not just the fingers.
- **Lift with the Legs** - Lift with the legs to allow the body's powerful leg muscles to do the work. Flex the knees and hips, not the back. Avoid bending at the waist. Try to keep the back "straight" during the lift. Do not look down at the object during the lift - look up. Looking up helps "straighten" the position of the back for a safer lift.
- **Pivot - Do Not Twist** - Do not twist the body when moving objects that have already been lifted. Pivot the feet and turn the entire body in the direction of movement.

25.12 EMPLOYEE NOTICE

Employees who may be exposed to hazardous chemicals shall be informed of the exposure and shall have access to the workplace chemical list and material safety data sheet (MSDS) for the hazardous chemicals. Employees, on request, shall be provided a copy of a specific MSDS with any trade secret information deleted. In addition, employees shall receive training concerning the hazards of the chemicals and measures they can take to protect themselves from those hazards. Employees shall be provided with appropriate personal protective equipment. These rights are guaranteed.

25.13 RIGHTS OF EMPLOYEES

The Agency may not discharge, cause to be discharged, otherwise discipline, or in any manner discriminate against an employee because the employee has:

- filed a complaint;
- assisted an inspector of the department who may make or is making an inspection under Section 502.011, Hazard Communication Act;
- instituted or caused to be instituted any proceeding under or related to this chapter;
- testified or is about to testify in a proceeding under this chapter; or
- exercised any rights afforded under this chapter on behalf of the employee or on behalf of others.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 25: SAFETY

Pay, position, seniority, or other benefits may not be lost as the result of the exercise of any right provided by this chapter.

A waiver by an employee of the benefits or requirements of this chapter is void. An employer's request or requirement that an employee waive any rights under this chapter as a condition of employment is a violation of this chapter.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 26: NOTARIES WITHOUT BOND

26.0 GENERAL

Employees that will perform notarizations as part of their job duties may apply to be commissioned as notaries public without bond. Employees that qualify as notaries without a bond are prohibited from providing notarial services outside of official state duties.

26.1 QUALIFICATION

An employee seeking to be commissioned as a notary public without bond must obtain approval from the employee's section/division director and must meet the eligibility requirements for appointment as a Texas notary public.

Upon approval by the section/division director to perform job-related notarizations, the employee must:

1. View the Notary Public Training Video (available on the Agency's website);
2. Print the Certificate of Completion provided at the end of the notary training video, which constitutes evidence of training on the duties and responsibilities of a Texas notary public and shall be filed in the employee's personnel file;
3. Complete [Form 2301-NB](#) (Application for Appointment as a Notary Public Without Bond); and
4. Complete [SORM-Form 203](#) (State Employee Notary Acknowledgment Form).

The employee shall forward aforementioned documents along with a Purchase Requisition to the Purchasing Section. Upon receipt of the required documents, the Purchasing Section will forward to the State Office of Risk Management (SORM) the following:

- Form 2301-NB;
- SORM Form 203; and
- An inter-agency transfer voucher (ITV) payable to the Secretary of State. The employee's name shall appear in the descriptive legal text section.

Once SORM has completed the verification certificate, the application and ITV will be forwarded to the Notary Public Unit for processing. The Notary Public Unit shall commission the employee if:

- The employee meets the eligibility requirements;
- The employee submits:
 1. a properly completed and executed application verified by SORM;
 2. the statement of officer and oath of office required by Article XVI, §1 Texas Constitution;
 3. the ITV in payment of fees required by §406.007(a)(2) and §406.007(b), Government Code; and
- No good cause exists for rejecting the application.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 26: NOTARIES WITHOUT BOND

The process is the same for an employee, already commissioned as a notary public without bond, seeking to renew the commission.

26.2 NOTARY SUPPLIES

Notary supplies must be kept in a safe and secure manner and shall only be used by the notary to whom they belong.

26.3 NOTARY STAMP

Once an employee is commissioned or re-commissioned as a notary public without bond, the Agency will provide the notary with a stamp to be used on all documents notarized as part of the notary's official state duties. The stamp shall comply with the requirements of Texas Government Code §406.013 and shall contain an additional line reading "*Notary without Bond.*"

26.4 NOTARY RECORD BOOK

The Agency will also provide a notary record book to every employee commissioned as a notary public without bond. For every notarization performed, the notary is required to record in the record book the information required by §406.014 of the Texas Government Code. Record books are required to be retained in accordance with Chapter 87 of the Texas Administrative Code. New record books may be obtained from Purchasing when needed.

26.5 PERFORMING NOTARIZATIONS

An employee who is commissioned as a notary without a bond is prohibited from providing notarial services outside of the employee's official state duties. If notarizing documents for the general public as part of the employee's duties, the employee may provide such notarial services, as long as they do not interfere with the employee's other job duties. An employee should consult with the employee's manager/team leader regarding the appropriate circumstances under which notarial services may be performed.

Each notary must follow the proper procedures for every notarization performed, including requiring personal appearance, obtaining sufficient identification, completing and executing the notarial certificate, and recording the required information about the notarization in the record book.

26.6 TRANSFER OR TERMINATION OF EMPLOYMENT OF NOTARIES WITHOUT BOND

When an employee who is commissioned as a notary without bond transfers employment to or from this Agency, the HRD will forward [SORM Form 204](#) to SORM.

When an employee of this Agency who is commissioned as a notary without bond terminates state employment, the HRD shall inform the employee that the employee must either:

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 26: NOTARIES WITHOUT BOND

- voluntarily surrender the notary public commission by submitting Form 2303 (Voluntary Surrender of Notary Public Commission) to the Notary Unit;
- Purchase and provide evidence of a bond to the Notary Public Unit for the time remaining on the notary's current term of office; or
- Apply for a new term of office by following the procedures for qualification.

The employee must surrender to HRD the notary stamp purchased and provided by the Agency. The employee shall retain the notary record book. If the employee intends to vacate the office of notary public the employee shall send the record book to the county clerk of the county in which the employee resides.

The HRD will forward [SORM Form 204](#) to SORM.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 27: SOCIAL MEDIA

27.0 OVERVIEW

Social media is an increasingly popular and effective communication tool. Platforms including, but not limited to, blogs (such as Blogger, WordPress, TypePad), social networking (Facebook, LinkedIn), social bookmarking (Delicious, StumbleUpon), news sharing (Digg, Yahoo!, Buzz), and photo and video sharing sites (Flickr, Vimeo, YouTube) provide the ability to communicate directly with the public, while promoting two-way communication to enhance understanding. As such, the Agency may utilize social media to supplement traditional communication efforts.

This policy is intended to ensure that official Agency messages are timely, accurate, and credible and that personal opinions are not misinterpreted as official agency positions. This policy also provides guidelines for an employee's use of social media both on and off duty

27.1 APPROVALS REQUIRED TO USE SOCIAL MEDIA FOR AGENCY BUSINESS

The decision to use a social media (including, but not limited to, Facebook, MySpace, LinkedIn, YouTube, and Twitter) for agency purposes must be evaluated and approved by the Deputy Secretary of State.

Information to be posted must be approved by the Director of Communications or the Deputy Director of Communications in consultation with the Executive Division and the appropriate division director, or designee.

Only individuals specifically authorized by the Director of Communications may post information to the agency social media platforms in the name of the Agency.

27.2 AUTHORIZED COMMUNICATIONS

All Agency-related social media communications will be conducted by authorized individuals in a professional, impartial, and politically neutral manner, in compliance with other Agency policy and procedures. Prior to posting, diligence should be made to ensure information that is posted is factual, accurate, and adheres to Agency policies, procedures, positions, and programs. In the event inaccurate or inappropriate information is posted, authorized personnel should correct or remove the postings as soon as feasible.

Individuals who are authorized to post information on behalf of the Agency will only address issues within the scope of their specific authorization and must adhere to the terms of service of the particular form of social media.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 27: SOCIAL MEDIA

27.3 ACCEPTABLE CONTENT

Social media posts will provide timely, accurate, and relevant information regarding Agency functions and programs. Social media communication on behalf of the Agency must be for the benefit of constituents, partners, and the Agency.

27.4 UNACCEPTABLE CONTENT

All published content is subject to monitoring. The Agency reserves the right to reject or remove content when the content is in violation of Agency policies. Postings or communications that contain any of the following forms of content will be subject to removal or rejection:

- Comments not topically related or relevant to the particular social medium article or subject matter being commented on;
- Comments in support of or in opposition to a political campaign, ballot measure, political party, or political candidate;
- Comments that contain profane, offensive, or obscene language or content;
- Comments that contain discriminatory, racist, inflammatory, unlawful, confidential, or otherwise objectionable statements, language, or content;
- Comments that engage in personal attacks of any kind or that use offensive terms that target an individual or group; or
- Comments that endorse or advertise a commercial product, service, or entity.

Social media sites hosted by the Agency will not contain or link to any site that contains the following types of information;

- Political views or partisan information;
- Discriminatory, racist, offensive, obscene, inflammatory, unlawful, or otherwise similarly objectionable statements, language, or content;
- Commercial endorsements or advertisements;
- Copyrighted information (Agency or otherwise) that may constitute an infringement of the rights of the copyright owner;
- Information that infringes on the privacy of others or is defamatory in nature;
- Information that is not open to the public; or
- Information prohibited by federal, state or local law.

27.5 RESPONSE TO QUESTIONS/COMMENTS

Responding to questions/comments from Agency social media site visitors is the responsibility of the Director of Communications and Deputy Director of Communications in consultation with the Executive Division and appropriate division directors, or designees. No other agency employees are permitted to post responses.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 27: SOCIAL MEDIA

27.6 POSTS AND COMMENTS ARE PUBLIC INFORMATION

Any written communication created or received by a state agency may be a public record subject to the Texas Public Information Act. Persons accessing social media sites used by the Agency should be aware that content submitted to or posted on the site by the Agency is public information and may be subject to disclosure to third parties under the Texas Public Information Act. Agency social media sites will include a statement to this effect.

27.7 INFORMATION REQUESTS

Requesters seeking information already accessible on Secretary of State Office websites will be provided a link to the information.

Information that was not created for public distribution requires an open records request before release. Requests submitted through social media platforms are not valid open records requests. Citizens initiating open records requests will be directed to the Secretary of State Office website email to submit a valid request.

27.8 RECORDS RETENTION

Social media content will be archived and retained for the required period of time in accordance with the Agency's records retention schedule.

27.9 EMPLOYEE USE OF SOCIAL MEDIA

Access to social media sites via state equipment (including state-owned computers, portable Internet capable devices, state email accounts, or any other state property) will remain restricted to only those employees that have a business reason to visit the sites. Access must be approved by the appropriate division director, the Director of the Information Technology Division, and the Director of Communications.

Agency policy applies in the virtual Internet environment the same as it does in the real world. Employees accessing agency social media sites via state computers, portable Internet capable devices, state email accounts or any other state property must conduct themselves in adherence with all Agency policies and procedures (including Human Resources, Ethics, and Information Security policies).

27.10 PERSONAL USE

Employees maintaining, establishing, or accessing personal social media accounts may not use state equipment (including state-owned computers, portable Internet capable devices, state email accounts, or any other state property) for non-work related purposes.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 27: SOCIAL MEDIA

Employees' conduct on personal social media accounts may be addressed by Agency management to the same extent as other types of outside conduct by employees.

Employees who engage in social media on their personal time:

- Must not imply or appear in any way to represent the Agency when acting in a personal capacity. This includes comments on an employee's job performance.
- Should not conduct themselves in such a way that their actions and relationships with each other interfere with or damage work relationships, and disrupt the flow of work.
- Should avoid becoming "friends" with their team leader/manager on FaceBook.
- Must include a disclaimer that their views do not represent the positions, strategies, or opinions of the Agency in any postings on any social media sites on which they are identified as an employee of the Agency, whether the site belongs to the Agency or not. An appropriate disclaimer would be similar to the following:

"This contains the thoughts and opinions of (employee name) and does not represent an official policy, position, or opinion of the Office of the Texas Secretary of State. Nothing herein should be attributed to the Office of the Texas Secretary of State."

- Should have no expectation of privacy when using social media sites. As such, employees are strongly encouraged to review the security settings on their personal social media sites to limit personal information that can be viewed.
- Should understand social media blurs the line between public and private communications. As such, employees are encouraged to make sure content in their personal social media profiles is not in conflict with professional standards of the Agency.
- Should realize that electronic communications may still exist – and thus be accessible – long after they are deleted from a computer. As such, employees are encouraged to be responsible and judicious in all social media postings and exchanges.
- Can be disciplined by the Agency for commentary, content, or images that are defamatory, pornographic, proprietary, harassing, libelous, confidential, or that can create a hostile work environment.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 28: UNEMPLOYMENT AND WORKERS' COMPENSATION

28.0 UNEMPLOYMENT COMPENSATION

With few exceptions, Agency employees are covered by the Texas Unemployment Compensation Act, which is posted in the HRD.

28.1 WORKERS' COMPENSATION

Agency employees are covered by the Texas Workers' Compensation Act (posted in the HRD) for occupational illness, disease, or injuries sustained in the course and scope of employment. Employees should immediately report any injury or disability of this kind to their manager/team leader and to the Worker's Compensation Claims Coordinator.

Employees can also contact the Office of Injured Employee Counsel regarding Injured Employee Rights and Responsibilities.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 29: Indoor Air Quality

29.0 Indoor Air Quality

Complaints about indoor air quality (IAQ) range from simple complaints from comfort issues (too hot/cold/drafty, etc.) and odd smells, to more complex problems where the air quality may be suspected of causing illness and lost work time.

It may not be easy to identify a single reason for IAQ complaints because of the number and variety of possible sources, causes, and varying individual sensitivities. Nevertheless, the Office of the Secretary of State (SOS) is committed to providing its employees and visitors an indoor environment free of contaminants.

29.1 IAQ Coordinator

The IAQ Coordinator (the Manager of Purchasing) is responsible for managing the Indoor Air Quality Management Program of the Agency. The IAQ Coordinator's responsibilities include:

- May train employees about the recognition, prevention, and resolution of IAQ problems;
- Submits/reports problems to Texas Facilities Commission (TFC) via their web portal building requests;
- May participate in ongoing state training; and
- Maintains IAQ records.
 - IAQ records include: IAQ complaints and resolutions, and documentation of any maintenance, repair, or remodeling activity that could adversely impact indoor air quality.

29.2 Conducting periodic walkthroughs to assess the current IAQ situation

The IAQ coordinator or designate conducts periodic walkthrough inspections in SOS-occupied areas. Mechanical rooms are assessed by the TFC building manager (upon request). During the walkthrough, IAQ problem indicators are checked and noted on a floor plan or comparable drawing, including:

- Unusual Odors;
- Dirty or unsanitary conditions;
- Visible fungal growth or mold;
- Evident moisture in inappropriate locations (e.g., moisture on walls, floors, or carpets);
- Staining or discoloration of building material(s);
- Smoke damage;
- Presence of hazardous substances;
- Unusual odors from equipment;

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

SECTION 29: Indoor Air Quality

- Personal air cleaners (e.g., ozone generators, portable filtration units), fans or heaters;
- Inadequate ventilation; and
- Blocked vents.

29.3 HVAC System

The condition and operations of the HVAC system are inspected by TFC, upon request.

29.4 Existing and Potential IAQ Problems

The IAQ Coordinator and TFC conduct an ongoing assessment of agency occupied buildings for existing problems. Identified IAQ problems are corrected and steps are taken to control them.

29.5 Smoking

Smoking is prohibited in all buildings occupied by the SOS.

29.6 Maintaining Cooperative Relations with Occupants

The IAQ Coordinator keeps occupants informed about building conditions and policies that may impact IAQ. Additionally, occupants are notified about planned major renovation, remodeling, maintenance or pest control activities.

29.7 Procedures for Responding to IAQ Complaints

- IAQ problems reported to Purchasing are logged into TFC's work-request system;
- The capability of in-house staff to respond to complaints is assessed and assistance provided if necessary; and
- Appropriate outside sources of assistance are identified, if applicable.

**OFFICE OF THE SECRETARY OF STATE
POLICIES AND PROCEDURES MANUAL**

Appendices

Appendix A [Forms](#)

Appendix B [Information Security Agreement](#)

Appendix C Training Matrix

**Office of the Secretary of State
Training Matrix**

Job Category	New Hire Training							Every Two Years					As Required by Certification	
	Training Checklist	Initial Performance Goals	EEO Training	Ethics Training	New Employee Orientation	Safety Training	Mindleaders	Info Security Policy	EEO Training	Ethics Training	Notification of Comp. Time Policy	Notification of HIV/AIDS Policy	Substance Abuse Free Workplace Training	Professional Recertification
Officials			X	X	X	X		X	X	X	X	X	X	
Directors, Managers			X	X	X	X		X	X	X	X	X	X	
Team Leaders	X	X	X	X	X	X	X	X	X	X	X	X	X	
Support Staff	X	X	X	X	X	X		X	X	X	X	X	X	
Professional Certifications														X

Information Security Policy

Office of the Secretary of State

Revised Date: Oct 24, 2018

Section 1

Introduction <input checked="" type="checkbox"/> Approved	Purpose of this Policy <input checked="" type="checkbox"/> Approved	General Policy <input checked="" type="checkbox"/> Approved
Security Policy Development and Maintenance Policy <input checked="" type="checkbox"/> Approved	Security Policy Standards <input checked="" type="checkbox"/> Approved	Violations and Disciplinary Actions Policy <input checked="" type="checkbox"/> Approved

Section 2

Acceptable Use Policy <input checked="" type="checkbox"/> Approved	Account Management Policy <input checked="" type="checkbox"/> Approved	Data Classification Policy <input checked="" type="checkbox"/> Approved
Email Policy <input checked="" type="checkbox"/> Approved	Malicious Code Policy <input checked="" type="checkbox"/> Approved	Network Access Policy <input checked="" type="checkbox"/> Approved
Password Policy <input checked="" type="checkbox"/> Approved	Portable Computing Policy <input checked="" type="checkbox"/> Approved	Privacy Policy <input checked="" type="checkbox"/> Approved
Security Awareness Policy <input checked="" type="checkbox"/> Approved	Software Licensing Policy <input checked="" type="checkbox"/> Approved	Exception Policy <input checked="" type="checkbox"/> Approved

An internal email address, [Information Security](#), has been established for reporting information security issues.

The [Information Security Acknowledgement and Nondisclosure Agreement](#) is now available

Section 3

Administration/Special Access Policy <input checked="" type="checkbox"/> Approved	Backup/Disaster Recovery Policy <input checked="" type="checkbox"/> Approved	Change Management Policy <input checked="" type="checkbox"/> Approved
Incident Management Policy <input checked="" type="checkbox"/> Approved	Intrusion Detection Policy <input checked="" type="checkbox"/> Approved	Network Configuration Policy <input checked="" type="checkbox"/> Approved
Physical Access Security Policy <input checked="" type="checkbox"/> Approved	System Development Policy <input checked="" type="checkbox"/> Approved	Security Monitoring Policy <input checked="" type="checkbox"/> Approved
System Security Policy <input checked="" type="checkbox"/> Approved	Vendor Access Policy <input checked="" type="checkbox"/> Approved	Computer Security Breach Notification Policy <input checked="" type="checkbox"/> Approved

An internal email address, [Information Security](#), has been established for reporting information security issues.

The [Information Security Acknowledgement and Nondisclosure Agreement](#) is now available

INTRODUCTION

The possibility that electronic information could be lost, corrupted, diverted, or misused represents a real threat to mission performance for the Office of the Secretary of State (SOS) and other government agencies. Today, SOS is more dependent than ever on information technology. Information technology has gone from being important to being essential in the performance of these missions. However, even as SOS's dependence on information technology has grown, so too has the vulnerability of this technology and the range of external threats to it.

Information security is a key aspect of the interaction among many important societal issues—defense, terrorism, commerce, privacy, intellectual property rights, and computer crime. Information technology resources also consume a growing share of the State's budget and are becoming increasingly important to daily life. As a result, a considerable body of applicable policy is in place, consisting of laws, statutes, regulations, Executive Orders, and other directives. SOS's Information Security Program, as well as those of other agencies, must operate within this complex policy landscape to ensure that the State, and in particular, SOS meets its obligations to its citizens and customers. Providing for the security of information resources is not only a difficult technical challenge, it is also a human challenge. Ultimately information security is a human endeavor that depends heavily on the behavior of individual people.

PURPOSE OF THIS POLICY

By information security we mean protection of the Office of the Secretary of State's, hereinafter referred to as the **Agency**, data, applications, networks, and computer systems from unauthorized access, alteration, or destruction.

The purpose of the information security policy is:

- To establish an **Agency**-wide approach to information security.
- To prescribe mechanisms that help identify and prevent the compromise of information security and the misuse of **Agency** data, applications, networks and computer systems.
- To define mechanisms that protect the reputation of the **Agency** and allow the **Agency** to satisfy its legal and ethical responsibilities with regard to its networks' and computer systems' connectivity to worldwide networks.
- To prescribe an effective mechanism for responding to external complaints and queries about real or perceived non-compliance with this policy.

GENERAL POLICY

Throughout the document the terms *must* and *should* are used carefully. The term *must* is not negotiable; the term *should* is a goal for the **Agency**.

- The *Agency* will use a layered approach of overlapping controls, monitoring and authentication to ensure overall security of the *Agency*'s data, network and system resources.
- Security reviews of servers, firewalls, routers and monitoring platforms must be conducted on a regular basis. These reviews must include monitoring access logs and results of intrusion detection software, where it has been installed.
- Vulnerability and risk assessment tests of external network connections must be conducted on a regular basis. At a minimum, testing should be performed annually, but the sensitivity of the information secured may require that these tests be done more often.
- Education should be implemented to ensure that users understand data sensitivity issues, levels of confidentiality, and the mechanisms to protect the data. This should be tailored to the role of the individual: network administrator, system administrator, data custodian, and users.
- Violation of the Information Security Policy may result in disciplinary actions as authorized by the *Agency* in accordance with *Agency* and disciplinary policies, procedures, and codes of conduct.

Ownership

The Information Security Policies are owned by the *Agency* Information Resources Manager (**IRM**). The **IRM**, or designate, is the only authority that can approve modifications to the Security Policies.

Support Information

This Policy is supported by the Security Policy Standards.

Disciplinary Action

Violation of this policy may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of *Agency* information resources access privileges, as well as civil and criminal prosecution. Violations of this policy or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Policy of the *Agency*.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.1	Marlin Craig	02/22/18		Scott Brandt	03/05/18

Security Policy Development and Maintenance Policy

Introduction

The *Agency* Information Security Policies provides the operational detail required for the successful implementation of the Information Security Program. These security policies were developed based on, and cross referenced to, the Security Policy Standards. In addition these policies have been developed by interpreting Health Insurance Portability and Accountability Act of 1996 (HIPAA), Texas Administrative Code, Chapter 202 (TAC 202) and other legislation and legal requirements, understanding business needs, evaluating existing technical implementations, and by considering the cultural environment.

Purpose

The business, technical, cultural, and legal environment of *Agency*, as it relates to information resources use and security, is constantly changing. These policies are technology neutral and apply to all aspects of information resources. Emerging technologies or new legislation, however, will impact these Information Security Policies over time. The Security Policies will be revised as needed to comply with changes in federal or state law or rules promulgated there under or to enhance its effectiveness.

Security Policy Development and Maintenance Policy

A number of factors could result in the need or desire to change the Security Policies. These factors include, but are not limited to:

- Review schedule
- New federal or state legislation
- Newly discovered security vulnerability
- New technology
- Audit report
- Business requirements
- Cost/benefit analysis
- Cultural change

Updates to the *Agency* Information Security Policies, which include establishing new policies, modifying existing policies, or removing policies, can result from three different processes:

- At least annually, the Information Security Officer (**ISO**), or designee, will review the Policies for possible addition, revision, or deletion. An addition, revision, or deletion is created if it is deemed appropriate.
- Every time new information resource technology is introduced into the *Agency*, a security assessment should be completed. The result of the security assessment could necessitate changes to the Security Policies before the new technology is permitted for use at the *Agency*.

Any User may propose the establishment, revision, or deletion of any practice standard at any time. These proposals should be directed to the **ISO** who will evaluate the proposal and make recommendations to the Information Resource Manager (**IRM**).

Once a change to the Security Policies has been approved by the **IRM**, or designee, the following steps will be taken as appropriate to properly document and communicate the change:

- The appropriate **IT** Security web pages will be updated with the change
- Training and compliance materials will be updated to reflect the change

The changes will be communicated using standard *Agency* communications methods such as: announcements, web page notification, newsletters, and communications meetings.

Support Information

This Policy is supported by the Security Policy Standard.

Disciplinary Action

Violation of this policy may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of *Agency* information resources access privileges, as well as civil and criminal prosecution. Violations of this policy or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Policy of the Agency.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.1	Marlin Craig	02/22/18		Scott Brandt	03/05/18

SECURITY POLICY STANDARDS

Introduction

The Information Security Policy Standards apply to all information obtained, created, or maintained by the *Agency's* automated Information Technology. These Policy Standards are based on the interpretation of Texas Administrative Code, Title 1, Part 10, Chapter 202 (TAC 202) and other reference material and apply equally to all levels of management and to the personnel they supervise. Further, these Policy Standards apply to all information generated by the *Agency's* Information Technology functions, through the time of its transfer to ownership external to the *Agency* or its proper disposal/destruction.

Audience

These Policy Standards apply equally to all personnel including, but not limited to, the *Agency's* employees, agents, consultants, volunteers, and all other authorized users granted access to information resources.

Definitions

Information: Any and all data, regardless of form, that is created, contained in, or processed by, Information Technology facilities, communications networks, or storage media.

Information Resources: any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, servers, personal computers, notebook computers, hand-held computers, personal digital assistants (PDA), USBs, distributed processing systems, network attached and computer controlled equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Key Roles & Responsibilities

Information Resources Manager (IRM): Responsible to the Secretary of State and the State of Texas for management of the *Agency's* information resources. The designation of an *Agency* IRM is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the state *Agency's* information activities, and ensure greater visibility of such activities within and between state agencies. The IRM has been given the authority and the accountability by the State of Texas to implement Security Policies, Procedures, Practice Standards, and Guidelines to protect the information resources of the *Agency*.

Information Security Officer (ISO): Responsible to the IRM for administering the information security function within the *Agency*. The ISO is the *Agency's* internal and external point of contact for all information security matters. The ISO duties include but are not limited to:

- Assuring the information security policy is updated on a regular basis (at a minimum annually) and published as appropriate.
- Appropriate training is provided to data owners, data custodians, network and system administrators, and users.

- Appoints a person, if applicable, to be responsible for security implementation, incident response, periodic user access reviews, and education of information security policies including, for example, information about virus infection risks.

Technology Management Team (TMT) Designated as a coordinating group comprised of information personnel from the *Agency*, chaired by the **IRM** and chartered with the task to establish procedures to implement these policies within their areas of responsibility, and for monitoring compliance.

Program Manager: Assigned information resource ownership; responsible for the information used in carrying out program(s) under their direction and provides appropriate direction to implement defined security controls and procedures.

Technical Manager (TM): Assigned custodians of information resources; provide technical facilities and support services to owners and users of information. **TM's** assist Program Management in the selection of cost effective controls used to protect information resources. **TM's** are charged with executing the monitoring techniques and procedures for detecting, reporting, and investigating breaches in information asset security.

Owner: The manager or agent responsible for the function which is supported by the resource, the individual upon whom responsibility rests for carrying out the program that uses the resources. The owner is responsible for establishing the controls that provide the security. The owner of a collection of information is the person responsible for the business results of that system or the use of the information. Where appropriate, ownership may be shared by managers of different departments.

Custodian: Guardian or caretaker; the holder of data, the agent charged with implementing the controls specified by the owner. The custodian is responsible for the processing and storage of information. For server applications Information Technology is the custodian; for micro and mini applications the owner or user may retain custodial responsibilities. The custodian is normally a provider of services.

User: Has the responsibility to (1) use the resource only for the purpose specified by the owner, (2) comply with controls established by the owner, and (3) prevent disclosure of confidential or sensitive information. The user is any person who has been authorized to read, enter, or update information by the owner of the information. The user is the single most effective control for providing adequate security.

Information Technology (IT): The name of the *Agency* department responsible for computers, networking, and data management.

Internal Auditor: Audits information security practices of the agency to determine if existing agency policies and procedures are followed. Audits information security practices of the agency to determine compliance with applicable laws. Makes recommendations to address any deficiencies.

System Administrator: Person responsible for the effective operation and maintenance of information resources, including implementation of standard procedures and controls to enforce an organization's security policy. Whereas each *Agency* will have one Information Security Officer, technical management may designate a number of system administrators.

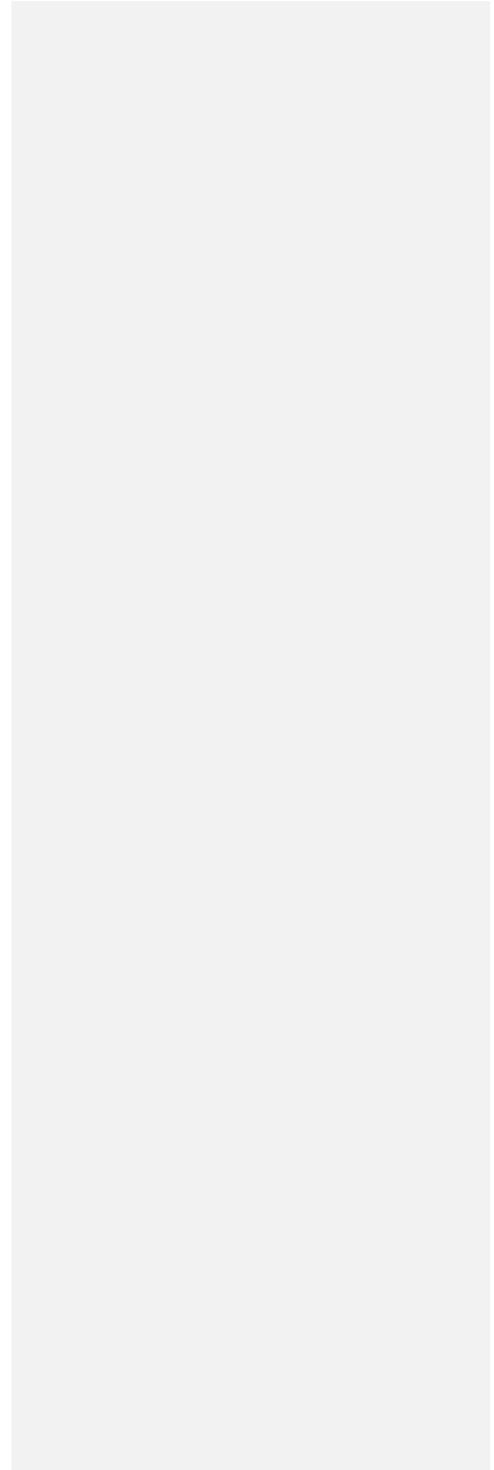
Application of Policy Standards

The *Agency* will protect the information resource assets of the Office of the Secretary of State and the state of Texas in accordance with the State of Texas Department of Information Resources' (DIR) Information Resources Security and Risk Management Policy, Standards and Guidelines as published in the Texas Administrative Code, Chapter 202, and as authorized by the Information Resources Management Act (Chapter 2054, Texas Government Code Annotated).

Specifically, the *Agency* will apply policies, procedures, practice standards, and guidelines to protect its **IT**

functions from internal data or programming errors and from misuse by individuals within or outside the *Agency*. This is to protect the *Agency* from the risk of compromising the integrity of state programs, violating individual rights to privacy and confidentiality, violating criminal law, or potentially endangering the public's safety.

All *Agency* information security programs will be responsive and adaptable to changing technologies affecting information resources.



Policy Standard Detail based on TAC 202 and Best Practices

Reference #

- 1** Information Technology Security controls must not be bypassed or disabled.
TAC 202.2 – (1)
- 2** Security awareness of personnel must be continually emphasized, reinforced, updated and validated.
TAC 202.8 – (d), (e)
- 3** All personnel are responsible for managing their use of information resources and are accountable for their actions relating to information resources security. Personnel are also equally responsible for reporting any suspected or confirmed violations of this policy to the appropriate management immediately.
TAC 202.2 – (3); TAC 202.3 – (c) (3)
- 4** Passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), and other computer systems security procedures and devices shall be protected by the individual user from use by, or disclosure to, any other individual or organization. All security violations shall be reported to the custodian or owner department management immediately.
TAC 202.2- (3); TAC 202.3 – (c) (3)
- 5** Access to, change to, and use of information resources must be strictly secured. Information access authority for each user must be reviewed on a regular basis, as well as at each job status change such as: a transfer, promotion, demotion, or termination of service.
TAC 202.3 - (c) (1)(A),(H); TAC 202.7 – (c) (2)
- 6** The use of information resources must be for officially authorized business purposes only. There is no guarantee of personal privacy or access to tools such as, but not limited to; email, Web browsing, and other electronic discussion tools. The use of these electronic communications tools may be monitored to fulfill complaint or investigation requirements. Departments responsible for the custody and operation of computers (custodian departments) shall be responsible for proper authorization of information resources utilization, the establishment of effective use, and reporting of performance to management.
TAC 202.2 – (3); TAC 202.7 – (h) (O), (j)

**Policy Standard, Detail based on TAC 202 and Best Practices
continued**

Reference #

- 7** Any data used in an information resources system must be kept confidential and secure by the user. The fact that the data may be stored electronically does not change the requirement to keep the information confidential and secure. Rather, the type of information or the information itself is the basis for determining whether the data must be kept confidential and secure. Furthermore, if this data is stored in a paper or electronic format, or if the data is copied, printed, or electronically transmitted the data must still be protected as confidential and secured.

TAC 202.2 – (1); TAC 202.3 – (c) (3); TAC 202.7 – (b)

- 8** All computer software programs, applications, source code, object code, documentation and data shall be guarded and protected as if it were state property.

TAC 202.2 – (1)

- 9** On termination of the relationship with the *Agency* users must surrender all property and information resources managed by the *Agency*. All security policies for information resources apply to and remain in force in the event of a terminated relationship until such surrender is made. Further, this policy survives the terminated relationship.

TAC 202.7 – (c) (2)

- 10** The owner must engage the **IRM**, or designate, at the onset of any project to acquire computer hardware or to purchase or develop computer software. The costs of acquisitions, development and operation of computer hardware and applications must be authorized by appropriate management. Management and the requesting department must act within their delegated approval limits in accordance with the *Agency* authorization policy. A list of standard software and hardware that may be obtained without specific, individual approval will be published.

Industry Best Practices

- 11** The department which requests and authorizes a computer application (the owner) must take the appropriate steps to ensure the integrity and security of all programs and data files created by, or acquired for, computer applications. To ensure a proper segregation of duties, owner responsibilities cannot be delegated to the custodian.

TAC 202.3 – (c) (1)

Policy Standard, continued Detail based on TAC 202 and Best Practices

Reference #

- 12** The information resource network is owned and controlled by **IT**. Approval must be obtained from **IT** before connecting a device that does not comply with published guidelines to the network. **IT** reserves the right to remove any network device that does not comply with standards or is not considered to be adequately secure.
Industry Best Practices
- 13** The sale or release of computer programs or data, including email lists and departmental telephone directories, to other persons or organizations must comply with all *Agency* legal and fiscal policies and procedures.
Industry Best Practices
- 14** The integrity of general use software, utilities, operating systems, networks, and respective data files are the responsibility of the custodian department. Data for test and research purposes must be de-personalized prior to release to testers unless each individual involved in the testing has authorized access to the data.
TAC 202.3 – (2), TAC 202.7 – (g) (1)
- 15** All changes or modifications to information resource systems, networks, programs or data must be approved by the owner department that is responsible for their integrity.
TAC 202.3 – (c) (1)
- 16** Custodian departments must provide adequate access controls in order to monitor systems to protect data and programs from misuse in accordance with the needs defined by owner departments. Access must be properly documented, authorized and controlled.
TAC 202.3 – (c) (2)
- 17** All departments must carefully assess the risk of unauthorized alteration, unauthorized disclosure, or loss of the data for which they are responsible and ensure, through the use of monitoring systems, that the *Agency* is protected from damage, monetary or otherwise. Owner and custodian departments must have appropriate backup and contingency plans for disaster recovery based on risk assessment and business requirements.
TAC 202.2 – (1); TAC 202.2 – (5); TAC 202.4 (a); TAC 202.6 (a) (5), (b); TAC 202.7 – (h) (D), (I), (P); 202.7 – (i) (1)

Policy Standard, Detail based on TAC 202 and Best Practices continued

Reference #

- 18** All computer systems contracts, leases, licenses, consulting arrangements or other agreements must be authorized and signed by an authorized *Agency* officer and must contain terms approved as to form by the Legal Department.
Industry Best Practices
- 19** Information resources computer systems and/or associated equipment used for *Agency* business that is conducted and managed outside of *Agency* control must meet contractual requirements and be subject to monitoring.
TAC 202.3 – (c) (2)
- 20** External access to and from information resources must meet appropriate published *Agency* security guidelines.
Industry Best Practices
- 21** All commercial software used on computer systems must be supported by a software license agreement that specifically describes the usage rights and restrictions of the product. Personnel must abide by all license agreements and must not illegally copy licensed software. The **IRM** through **IT** reserves the right to remove any unlicensed software from any computer system.
TAC 202.7 – (h) (S); Section 117 of the Copyright Act
- 22** The **IRM** through **IT** reserves the right to remove any non-business related software or files from any system. Examples of non-business related software or files include, but are not limited to: games, instant messengers, pop email, music files, image files, freeware, and shareware.
TAC 202.7 – (h) (S); Industry Best Practices
- 23** Adherence to all other policies, practice standards, procedures, and guidelines issued in support of these policy statements is mandatory.
Industry Best Practices

Disciplinary Action

Violation of this policy may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of *Agency* information resources access privileges, as well as civil and criminal prosecution. Violations of this policy or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Policy of the Agency.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.2	Scott Brandt	8/15/2018		Scott Brandt	8/15/2018

Violations and Disciplinary Actions Policy

Introduction

All **Agency** information resources are subject to certain rules and conditions concerning official and appropriate use as specified.

Purpose

Any event that results in theft, loss, unauthorized use, unauthorized disclosure, unauthorized modification, unauthorized destruction, or degraded or denied services of information resources constitutes a breach of security.

Violations Policy

Violations may include, but are not limited to any act that:

- exposes the **Agency** to actual or potential monetary loss through the compromise of information resources security,
- involves the disclosure of sensitive or confidential information or the unauthorized use of **Agency** data or resources,
- involves the use of information resources for personal gain, unethical, harmful, or illicit purposes, or results in public embarrassment to the **Agency**.

Disciplinary Actions Policy

Violations of these Information Security Policies may result in immediate disciplinary action that may include, but may not be limited to:

- formal reprimand,
- suspended or restricted access to **Agency** information resources,
- restitution or reimbursement for any damage or misappropriation of any **Agency** property,
- suspension without pay,
- termination of employment,
- termination of contract,
- civil prosecution or state and/or federal criminal prosecution.

Support Information

This Policy is supported by the Security Policy Standard.

Disciplinary Action

Violation of this policy may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of **Agency** information resources access privileges, as well as civil and criminal prosecution. Violations of this policy or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Policy of the Agency.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.1	Marlin Craig	02/22/18		Scott Brandt	03/05/18

ACCEPTABLE USE POLICY

Introduction

Under the provisions of the Information Resources Management Act, information resources are strategic assets of the State of Texas that must be managed as valuable state resources. Thus this policy is established to achieve the following:

- To ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources.
- To establish prudent and acceptable practices regarding the use of information resources.
- To educate individuals who may use information resources with respect to their responsibilities associated with such use.

Ownership of Electronic Files

Electronic files created, sent, received, or stored on information resources owned, leased administered, or otherwise under the custody and control of the *Agency* are the property of the *Agency*.

Privacy

Electronic files created, sent, received, or stored on information resources owned, leased, administered, or otherwise under the custody and control of the *Agency* are not private and may be accessed by *Agency IT* employees at any time without knowledge of the information resources user or owner. Electronic file content may be accessed by appropriate personnel in accordance with the provisions and safeguards provided in the Texas Administrative Code 202, Information Resource Standards.

Acceptable Use Policy

The *Agency* must have a policy on appropriate and acceptable use that includes these requirements:

- *Agency* computer resources must be used in a manner that complies with *Agency* policies and State and Federal laws and regulations. It is against *Agency* policy to install or run software requiring a license on any *Agency* computer without a valid license.
- All software must be authorized by the *Agency IT* prior to use. A list of authorized software will be maintained in Appendix A of this Policy. Individuals may request written approval for software use through the *Agency IRM*. Unauthorized software is subject to removal upon discovery.
- Use of the *Agency's* computing and networking infrastructure by *Agency* employees unrelated to their *Agency* positions must be limited in both time and resources and must not interfere in any way with *Agency* functions or the employee's duties. It is the responsibility of employees to consult their supervisors, if they have any questions in this respect.
- Uses that interfere with the proper functioning or the ability of others to make use of the *Agency's* networks, computer systems, applications and data resources are not permitted.
- Use of *Agency* computer resources for personal profit is not permitted.
- Files, images, emails or documents which may cause legal action against or embarrassment to the *Agency*, may not be sent, received, accessed in any format (i.e. auditory, verbal or visual), downloaded or stored on *Agency* information resources.
- All messages, files and documents – including personal messages, files and documents – located on *Agency* information resources are owned by the *Agency*, may be subject to open records requests, and may be accessed in accordance with this policy.

- Decryption of passwords is not permitted, except by authorized staff performing security reviews or investigations.
- Use of network sniffers shall be restricted to system administrators who must use such tools to solve network problems. Network sniffers may be used by auditors or security officers in the performance of their duties. All use of network sniffers shall be approved by the **IRM**. They must not be used to monitor or track any individual's network activity except under special authorization as defined by **Agency** policy that protects the privacy of information in electronic form.
- Users must not download, install or run any programs or utilities on their systems except those authorized and installed by the **Agency IT** and specifically designed to conduct the business of the **Agency**. Examples of non-business related software or files include, but are not limited to: unauthorized peer-to-peer (P2P) file-sharing software, games, unauthorized instant messengers (IM), pop email, music files, image files, freeware, and shareware. Unauthorized software may be removed upon discovery.

Incidental Use

As a convenience to the **Agency** user community, incidental use of information resources may be permitted. The following restrictions apply:

- Incidental use must not interfere with the normal performance of an employee's work duties.
- Storage of personal email messages, voice messages, files and documents within **Agency's** information resources must be nominal.
- All messages, files and documents – including personal messages, files and documents – located on **Agency** information resources are owned by **Agency**, may be subject to open records requests, and may be accessed in accordance with this policy.

Support Information

This Policy is supported by the Security Policy Standard.

Disciplinary Action

Violation of this policy may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of **Agency** information resources access privileges, as well as civil and criminal prosecution. Violations of this policy or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Policy of the Agency.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.1	Marlin Craig	02/22/18		Scott Brandt	03/05/18

Appendix A to the Acceptable Use Policy

Approved Agency Software

Approved *Agency* Software is comprised of three categories; Level I, Level II, and Level III as listed and defined below:

Agency Level I Software

Operating Systems, networking and application software which is *Agency* licensed, fully supported, and IT pre-installed (imaged) on all *Agency* workstations.

- Windows 7
- Firefox
- Chrome
- Silverlight
- Adobe Reader
- Office 2013
- Office 2016
- Oracle Client
- Novell Client
- FireEye
- Malware Bytes
- BitDefender Anti-virus
- SCCM Client

Agency Level II software

Application software which is IT installed, fully supported and *Agency* licensed on an as needed basis for requested *Agency* workstations. **Level II** software requires a written Supervisor/Team Leader authorization request to the *Agency IRM* for approval prior to installation.

- SQL Navigator
- TOAD
- Eclipse
- Visual Studio
- MS Project
- MS Visio
- Oracle Virtual Box
- Web Trends
- Adobe C3
- Dreamweaver
- Arbor Text
- Crystal Reports
- Typing Master
- Walz Mailer
- Putty
- Card Scan
- Textpad

Skype
Webex
gotomypc
Filezilla
winscp
notepad++
xming
openvpn client
jenkins
jasper
ant
maven

Agency Level III Software

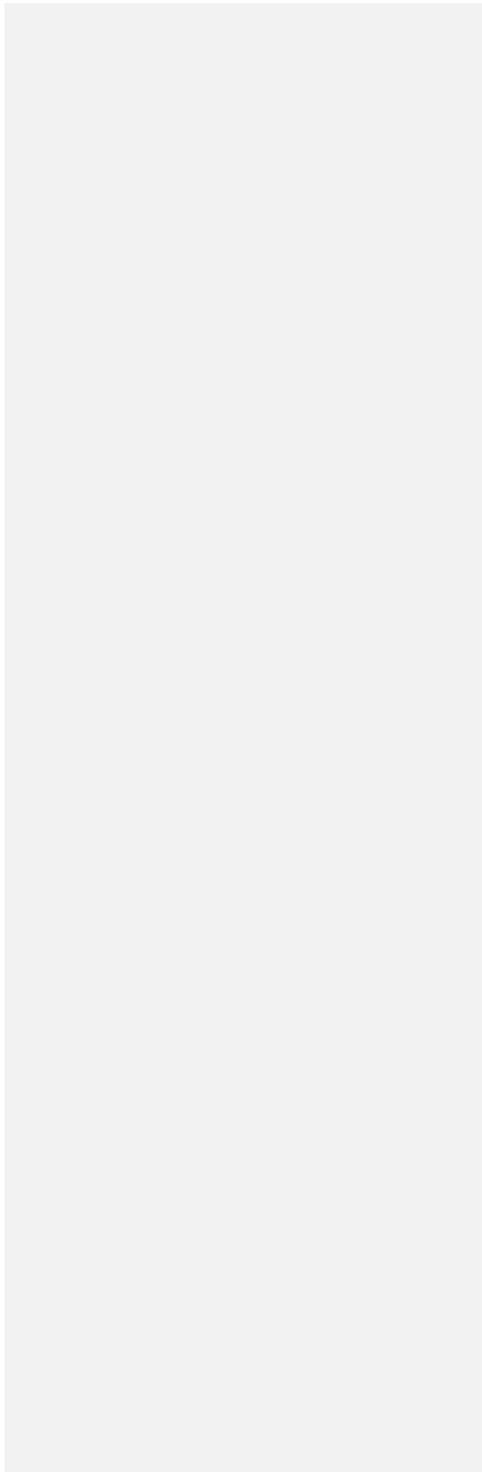
Application software which IT verifies the license, installs the software on requested *Agency* workstations, but is not IT supported (personal production/organizational software i.e. an individually purchased Palm Pilot or Blackberry). If there is an issue with the installation of **Level III** software or the workstation performance after the installation, the workstation will be re-imaged.

Level III software requires a written Supervisor/Team Leader authorization request to the *Agency IRM* for approval prior to installation.

Secure CRT
Wireshark
WebInspect
CoreImpact
Nessus

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.6	Scott Brandt	02/22/18		Scott Brandt	03/05/18



ACCOUNT MANAGEMENT POLICY

Introduction

Computer accounts are the means used to grant access to *Agency* information resources. These accounts provide a means of providing accountability, a key to any computer security program, for Information Technology usage. This means that creating, controlling, and monitoring all computer accounts is extremely important to an overall security program.

Purpose

The purpose of the *Agency* Account Management Security Policy is to establish the rules for the creation, monitoring, control and removal of user accounts.

Account Management Policy

- All accounts created must have an associated request and approval that is appropriate for the *Agency* system or service.
- All users must sign the *Agency* Information Security Acknowledgement and Nondisclosure Agreement before access is given to an account.
- All accounts must be uniquely identifiable using the assigned user name.
- All default passwords for accounts must be constructed in accordance with the *Agency* Password Policy.
- All accounts must have a password expiration that complies with the *Agency* Password Policy.
- Accounts of individuals on extended leave (more than 30 days) will be disabled.
- All new user accounts that have not been accessed within 30 days of creation will be disabled.
- Supervisors are responsible for immediately notifying Information Security of individuals that change roles within *Agency* or are separated from their relationship with *Agency*
- System Administrators or other designated staff:
 - ❖ are responsible for removing the accounts of individuals that change roles within *Agency* or are separated from their relationship with *Agency*
 - ❖ must have a documented process to modify a user account to accommodate situations such as name changes, accounting changes and permission changes
 - ❖ must have a documented process for periodically reviewing existing accounts for validity
 - ❖ are subject to independent audit review
 - ❖ must provide a list of accounts for the systems they administer when requested by authorized *Agency* management
 - ❖ must cooperate with authorized *Agency* management investigating security incidents.

Support Information

This Policy is supported by the Security Policy Standard.

Disciplinary Action

Violation of this policy may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of *Agency* information resources access privileges, as well as civil and criminal prosecution. Violations of this policy or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Policy of the Agency.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.1	Marlin Craig	03/05/18		Scott Brandt	03/06/05

DATA CLASSIFICATION POLICY

Introduction

Agreed information security classification definitions are an essential pre-requisite for many information security policies. They provide a consistent method for assessing and applying a sensitivity level to the important information assets of the *Agency*. These classification "labels" can then be used as the basis for evaluating the appropriate protective measures (technical and non-technical) needed to ensure the risk to these assets is minimized.

Purpose

It is essential that all *Agency* data be protected. There are however gradations that require different levels of security. All data should be reviewed on a periodic basis and classified according to its use, sensitivity, and importance. To assure proper protection of the *Agency*'s information resources, various levels of classifications will be applied.

Data Classification Policy

The *Agency* has specified three classes below:

High Risk - Information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure. Data covered by federal and state legislation, such as FERPA, HIPAA or the Data Protection Act, are in this class. Payroll, personnel, and financial information are also in this class because of privacy requirements.

This policy recognizes that other data may need to be treated as high risk because it would cause severe damage to the *Agency* if disclosed or modified. The data owner should make this determination. It is the data owner's responsibility to implement the necessary security requirements.

Confidential – Data that would not expose the *Agency* to loss if disclosed, but that the data owner feels should be protected to prevent unauthorized disclosure. It is the data owner's responsibility to implement the necessary security requirements.

Public - Information that may be freely disseminated.

All information resources should be categorized and protected according to the requirements set for each classification. The data classification and its corresponding level of protection should be consistent when the data is replicated and as it flows through the *Agency*.

- Owners must determine the data classification and must ensure that the data custodian is protecting the data in a manner appropriate to its classification.
- No *Agency*-owned system or network subnet can have a connection to the Internet without the means to protect the information on those systems consistent with its confidentiality classification.
- Custodians are responsible for creating data repositories and data transfer procedures which protect data in the manner appropriate to its classification.
- High risk data must be encrypted during transmission over unsecure channels.
- Confidential data should be encrypted during transmission over unsecure channels.
- All appropriate data should be backed up, and the backups tested periodically, as part of a documented, regular process.

- When Technology assets have reached the end of their useful life they should be sent to the SOS Disposal Team for proper disposal.
- The SOS Disposal Team will securely erase or destroy all storage mediums in accordance with current industry best practices.
- Backups of data must be handled with the same security precautions as the data itself. When systems are disposed of, or repurposed, data must be certified deleted or disks destroyed consistent with industry best practices for the security level of the data.

Commented [MC1]: Added 22 May 22, 2017

Support Information

This Policy is supported by the Security Policy Standard.

Disciplinary Action

Violation of this policy may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of *Agency* information resources access privileges, as well as civil and criminal prosecution. Violations of this policy or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Policy of the Agency.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.2	Marlin Craig	05/02/18		Scott Brandt	03/05/18

E MAIL USE POLICY

Introduction

Under the provisions of the Information Resources Management Act, information resources are strategic assets of the State of Texas that must be managed as valuable state resources. Thus this policy is established to achieve the following:

- To ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources.
- To establish prudent and acceptable practices regarding the use of email.
- To educate individuals using email with respect to their responsibilities associated with such use.

Purpose

The purpose of the *Agency* Email Policy is to establish the rules for the use of *Agency* email for the sending, receiving, or storing of electronic mail.

Definitions

Electronic mail system: Any computer software application that allows electronic mail to be communicated from one computing system to another.

Electronic mail (email): Any message, image, form, attachment, data, or other communication sent, received, or stored within an electronic mail system.

Email Use Policy

- The following activities are prohibited by policy:
 - ❖ Sending email that is intimidating or harassing.
 - ❖ Using email for purposes of political lobbying or campaigning.
 - ❖ Violating copyright laws by inappropriately distributing protected works.
 - ❖ Posing as anyone other than oneself when sending email, except when authorized to send messages for another when serving in an administrative support role.
 - ❖ The use of unauthorized e-mail software.
 - ❖ Excessive personal use. Personal Use of email is a privilege which is revocable at any time.
- The following activities are prohibited because they impede the functioning of network communications and the efficient operations of electronic mail systems:
 - ❖ Sending or forwarding chain letters.
 - ❖ Sending unsolicited messages to large groups except as required to conduct *Agency* business.
 - ❖ Sending or forwarding email that is likely to contain computer viruses.
- All sensitive *Agency* material transmitted over external network must be encrypted.
- All user activity on *Agency* information resource assets is subject to logging and review.
- Electronic mail users must not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of *Agency* or any unit of the *Agency* unless appropriately authorized to do so. Where appropriate, an explicit disclaimer will be included unless it is clear from the context that the author is not representing the *Agency*. An example of a simple disclaimer is: "the opinions expressed are my own,

and not necessarily those of my employer."

- Individuals must not send, forward or receive confidential or sensitive *Agency* information through non-*Agency* email accounts. Examples of non-*Agency* email accounts include, but are not limited to: Hotmail, Yahoo mail, Goggle mail, AOL mail, and email provided by other Internet Service Providers (ISP).

Individuals must not send, forward, receive or store confidential or sensitive *Agency* information utilizing non-*Agency* accredited mobile devices. Examples of mobile devices include, but are not limited to: Personal Data Assistants, two-way pagers and cellular telephones.

Support Information

This Policy is supported by the Security Policy Standard.

Disciplinary Action

Violation of this policy may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of *Agency* information resources access privileges, as well as civil and criminal prosecution. Violations of this policy or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Policy of the Agency.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.1	Marlin Craig	02/20/18		Scott Brandt	03/05/18

MALICIOUS CODE POLICY

Introduction

The number of computer security and malicious code incidents linked with the resulting cost of business disruption and service restoration continue to escalate. Implementing solid security policies, blocking unnecessary access to networks and computers, improving user security awareness, and early detection and mitigation of security incidents are some of the actions that can be taken to reduce the risk and drive down the cost of security incidents.

Purpose

The purpose of the Malicious Code Policy is to describe the requirements for dealing with computer virus, spyware, worm and Trojan Horse prevention, detection and cleanup.

Malicious Code Policy

- The willful introduction of computer viruses or disruptive/destructive programs into the *Agency* environment is prohibited, and violators may be subject to prosecution.
- All workstation systems that connect to the network must be protected with an approved, licensed anti-virus software product that it is kept updated according to **IT**'s recommendations.
- All printers that connect to the network must only have necessary ports enabled according to **IT**'s recommendations.
- All servers that connect to the network and that are vulnerable to virus or worm attack must be protected with an approved, licensed anti-virus software product that it is kept updated. Every virus that is not automatically cleaned by the virus protection software constitutes a security incident and must be reported to the Help Desk.
- All incoming data including electronic mail must be scanned for viruses where such products exist and are financially feasible to implement. Outgoing electronic mail should be scanned where such capabilities exist.
- Where feasible, system or network administrators should inform users when a malicious code threat has been detected.
- Virus scanning logs should be maintained whenever email is centrally scanned for viruses.
- Personal devices (phone, usb, tablets, laptops, external hard drives..) must not be connected to the SOS network, or connected to SOS devices (PC, laptops, switches..).

Support Information

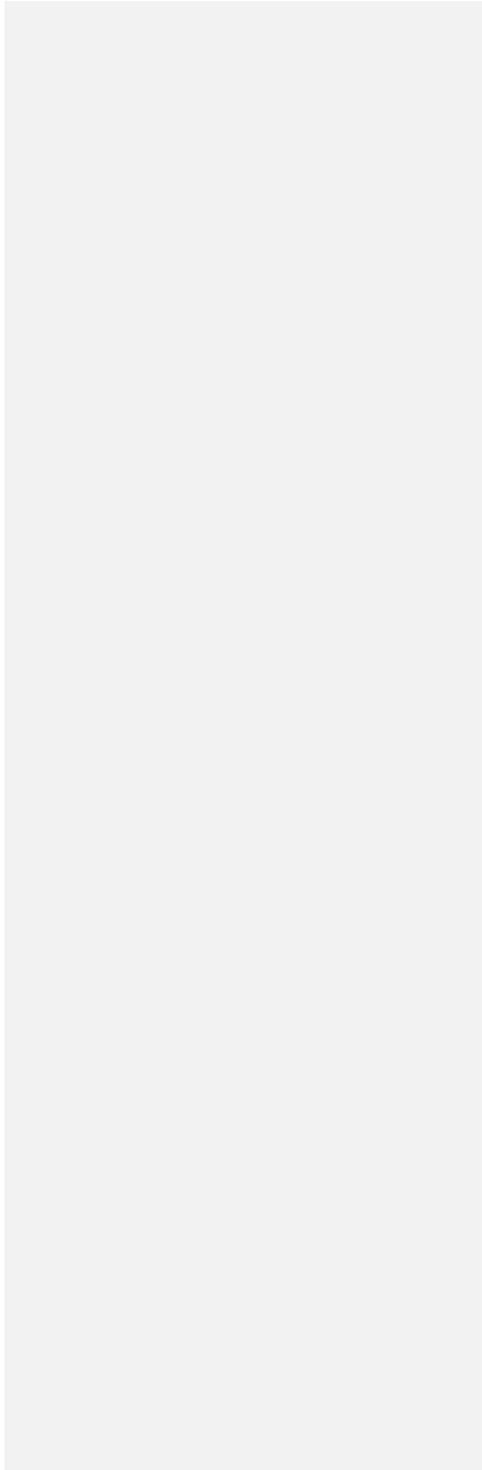
This Policy is supported by the Security Policy Standard.

Disciplinary Action

Violation of this policy may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of *Agency* information resources access privileges, as well as civil and criminal prosecution. Violations of this policy or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Policy of the Agency.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.2	Marlin Craig	08/15/18		Scott Brandt	08/15/18



NETWORK ACCESS POLICY

Introduction

The *Agency* network infrastructure is provided as a central utility for all users of *Agency* information resources. It is important that the infrastructure, which includes cabling and the associated 'active equipment', continues to develop with sufficient flexibility to meet *Agency* demands while at the same time remaining capable of exploiting anticipated developments in high speed networking technology to allow the future provision of enhanced user services.

Purpose

The purpose of the *Agency* Network Access Policy is to establish the rules for the access and use of the network infrastructure. These rules are necessary to preserve the integrity, availability and confidentiality of *Agency* information.

Network Access Policy

- Users are permitted to use only those network addresses issued to them by *Agency IT*.
- All remote access to *Agency* will be either through an approved VPN software(gotomypc) or via an approved Internet Service Provider (ISP).
- Remote users may connect to *Agency* information resources only through methods and using protocols approved by *Agency*.
- Users inside the *Agency* firewall may not be connected to the *Agency* network at the same time a modem is being used to connect to an external network.
- Users must not install network hardware or software that provides network services without written approval from the *IRM*. This includes wireless access points, modems, and remote access software.
- Non *Agency* computer systems that require network connectivity must conform to *Agency IT* Standards, and get approval from *IRM* or *ISO*.
- Users must not download, install or run security programs or utilities that reveal weaknesses in the security of a system. For example, *Agency* users must not run password cracking programs, packet sniffers, network mapping tools, or port scanners while connected in any manner to the *Agency* network infrastructure without written approval from the *IRM*.
- Users are not permitted to alter network hardware in any way.

Support Information

This Policy is supported by the Security Policy Standard.

Disciplinary Action

Violation of this policy may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of *Agency* information resources access privileges, as well as civil and criminal prosecution. Violations of this policy or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Policy of the Agency.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.1	Marlin Craig	02/20/18		Scott Brandt	03/05/18

PASSWORD POLICY

Introduction

User authentication is a means to control who has access to an Information Technology system. Controlling the access is necessary for any information resource. Access gained by an unauthorized entity can cause loss of information confidentiality, integrity and availability that may result in loss of revenue, liability, loss of trust, or embarrassment to the *Agency*.

Three factors, or a combination of these factors, can be used to authenticate a user. Examples are:

- Something you know – password, Personal Identification Number (PIN)
- Something you have – Smartcard
- Something you are – fingerprint, iris scan, voice

A combination of factors – Smartcard and a PIN

Purpose

The purpose of the *Agency* Password Policy is to establish the rules for the creation, distribution, safeguarding, termination, and reclamation of the *Agency* user authentication mechanisms.

Password Policy

- All passwords, including initial passwords, must be constructed and implemented according to the following *Agency* Information Technology rules:
 - ❖ it must adhere to a minimum password standard as established by Appendix A of this Policy
 - ❖ it must be routinely changed to adhere to the password aging standard as established in Appendix A of this Policy
 - ❖ it must not be anything that can easily be tied back to the account owner such as: user name, social security number, nickname, relative's names, birth date, etc.
 - ❖ it must not be dictionary words or acronyms
 - ❖ password history must be kept to prevent the reuse of a password
- Stored passwords must be encrypted.
- User account passwords must not be divulged to anyone. *Agency* IT and IT contractors must not ask for user account passwords. All passwords are to be treated as sensitive, Confidential SOS information.
- Do not use the "Remember Password" feature for critical systems/applications (for example, servers, applications with sensitive information and network equipment).
- Security tokens (i.e. Smartcard) must be returned on demand or upon termination of the relationship with the *Agency*.
- Application passwords must support authentication of individual users, not groups.
- Applications must not store passwords in clear text or in any easily reversible form.
- Applications must not transmit passwords in clear text over the network.
- If the security of a password is in doubt, the password must be changed immediately.
- Administrators must not circumvent the Password Policy for the sake of ease of use.
- Users must not circumvent password entry with auto logon, application remembering, embedded scripts or hard coded passwords in client software. Exceptions may be made for specific applications (like automated backup) with the approval of the *Agency* ISO. In order for an exception to be approved there must be a procedure to change the passwords.
- Computing devices must not be left unattended without enabling a password protected screensaver or

Commented [MC2]: Added may 2017

Commented [MC3]: Added 22 May 2017

logging off of the device.

- **IT Helpdesk password change procedures must include the following:**
 - ❖ authenticate the user to the helpdesk before changing password
 - ❖ change to a strong password
 - ❖ the user must change password at first login
- In the event passwords are found or discovered, the following steps must be taken:
 - ❖ Take control of the passwords and protect them
 - ❖ Report the discovery to the *Agency* ISO
 - ❖ Transfer the passwords to an authorized person as directed by the *Agency* ISO

Support Information

This Policy is supported by the Security Policy Standard.

Disciplinary Action

Violation of this policy may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of *Agency* information resources access privileges, as well as civil and criminal prosecution. Violations of this policy or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Policy of the Agency.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.2	Marlin Craig	02/22/18		Scott Brandt	03/05/18

Appendix A to the Password Policy

Agency minimum password standard

The following minimum standard for password creation applies to users of *Agency* information systems.

Use a minimum of eight characters and a combination of alpha and numeric characters. Administrator accounts must use a minimum of fourteen characters and a combination of alpha and numeric characters.

Users are encouraged to use a more complex password structure including at least one character from the following four classes:

- English upper case letters
 - English lower case letters
 - Numerals (0,1,2,...)
 - Non-alphanumeric (special) characters such as punctuation symbols (!@#%&* +=?/~`;; <>|).
- Very important passwords (e.g. password for any privileged or administrative account) should be at least 14 characters long;
 - Do not base PIN or passwords on any of the following details:
 - Months of the year, days of the week or any other aspect of the calendar;
 - Family names, initials or car registration numbers;
 - A proper name or any word in the dictionary without altering it in some way;
 - Can be derived from a dictionary word, e.g. by reversing letters;
 - Department or faculty names, identifiers or references;
 - Telephone numbers or similar all numeric groups;
 - User ID, user name, group ID or other system identifier;
 - More than two consecutive identical characters;
 - All-numeric or all-alphabetic groups;
 - Obvious phrases or sequences such as "SOS123" or "123456";

- Do not reuse a password: construct a new password each time it is changed.

The following strategies will help users to generate a password that is easy to remember, is hard to guess and complies with the *Agency* policy.

- Use a mixture of upper and lower case, numerals and punctuation e.g. **Keep0ut!**
- String several words or parts of words together e.g. **it'sCold**
- Choose a phrase, perhaps a line from a poem or song and form passwords by concatenating words from the phrase along with digits and/or punctuation. e.g. **Tw1nkL3*** (from twinkle, twinkle, little star)
- Invent phrases like car registration plates e.g. **one4you!**

Agency password aging policy

- Passwords must be changed at least every 90 days

Agency account lockout policy

- An account lockout policy of three failed login attempts is in effect.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.2	Marlin Craig	10/24/18		Scott Brandt	10/24/18

PORTABLE COMPUTING POLICY

Introduction

Portable computing devices are becoming increasingly powerful and affordable. Their small size and functionality are making these devices ever more desirable to replace traditional desktop devices in a wide number of applications. However, the portability offered by these devices may increase the security exposure to groups using the devices.

Purpose

The purpose of the *Agency* Portable Computing Security Policy is to establish the rules for the use of mobile computing devices and their connection to the network. These rules are necessary to preserve the integrity, availability, and confidentiality of *Agency* information.

Definitions

Portable Computing Devices: Any easily portable device that is capable of receiving and/or transmitting data to and from *Agency* information resources. These include, but are not limited to, notebook computers, handheld computers, and cell phones.

Portable Computing Policy

- Only *Agency* approved portable computing devices may be used to access *Agency* information resources.
- Portable computing devices **must** be password protected.
- Sensitive *Agency* data should not be stored on portable computing devices. However, in the event that there is no alternative to local storage, all sensitive *Agency* data should be encrypted using approved encryption techniques.
- *Agency* data must not be transmitted via wireless to or from a portable computing device unless approved wireless transmission protocols along with approved encryption techniques are utilized.
- *Agency* mobile devices including, but not limited to PDA's and smart phones and will be used only for *agency* business and must be used in accordance to the guidelines established by *Appendix A* of this Policy.
- All remote access (dial in services) to the *Agency* network must be through an approved method as established in the network access policy.
- Non *agency* computer systems that require network connectivity must conform to *Agency* IT Standards and must be approved in writing by the *Agency* ISO. Unattended portable computing devices must be physically secure. This means they must be locked in an office, locked in a desk drawer or filing cabinet, or attached to a desk or cabinet via a cable lock system.

Support Information

This Policy is supported by the Security Policy Standard.

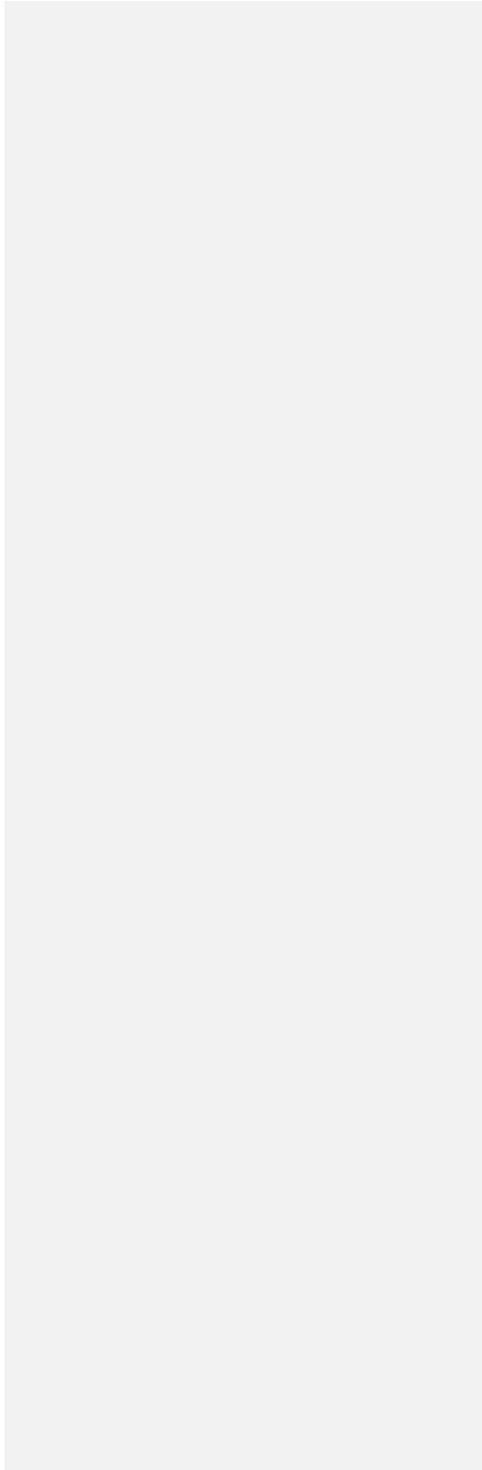
Disciplinary Action

Violation of this policy may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of *Agency* information resources access privileges, as well as civil and criminal

prosecution. Violations of this policy or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Policy of the Agency.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.3	Marlin Craig	2/19/2018		Scott Brandt	03/05/2018



Appendix A to PORTABLE COMPUTING POLICY

Agency Mobile Device Acceptable Use Policy

Agency mobile devices including but not limited to smart phones and tablets will be used only for Agency business. No personal email may be stored on agency devices.

All mobile devices must be password protected.

Agency owned devices will be connected via Agency approved access methods.

The following five requirements apply to Agency employees wishing to use a personal device to access your agency mail account:

- 1) employee must use Outlook Web Access or VPN access
- 2) employee must enable a pass code on the device
- 3) employee must enable the option to wipe the device after 10 failed attempts to enter the pass code
- 4) employee must agree that the agency may remotely wipe the entire contents of the device, including the employee's personal data, at the agency's sole discretion without advance notice to the employee
- 5) employee must receive written authorization from [Information Security](#) – which can be GRANTED based on compliance with requirements 1, 2, 3, and 4

Phone service may only be used to call another agency owned device. All SOS mobile devices are part of an agency pool of phone minutes. Calls between Agency owned devices do not impact the agency pool of minutes or accrue charges. All other phone calls will use minutes from the agency pool. Only users specifically authorized for additional phone services may initiate non-emergency calls to phone numbers other than to another agency owned mobile device.

Users must report lost or stolen mobile devices **IMMEDIATELY**. During normal business hours, the report should be made to the SOS Help Desk. After normal business hours and on weekends, lost or stolen devices should be reported to the IT Director or informationsecurity@sos.state.tx.us.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.5	Marlin Craig	1/06/2018		Scott Brandt	03/05/2018

PRIVACY POLICY

Introduction

Privacy Policies are mechanisms used to establish the limits and expectations for the users of *Agency* information resources. Internal users should have no expectation of privacy with respect to information resources.

Purpose

The purpose of the *Agency* Information Privacy Policy is to clearly communicate the *Agency* Information Technology privacy expectations to information resource users.

Definitions

Webserver: A computer that delivers (*serves up*) web pages.

Web page: A document on the World Wide Web. Every Web page is identified by a unique URL (Uniform Resource Locator).

World Wide Web: A system of Internet hosts that supports documents formatted in HTML (HyperText Markup Language) which contains links to other documents (hyperlinks) and to audio, video, and graphic images. Users can access the Web with special applications called browsers, such as Netscape Navigator, and Microsoft Internet Explorer.

Website: A location on the World Wide Web, accessed by typing its address (URL) into a Web browser. A Web site always includes a home page and may contain additional documents or pages.

Privacy Policy

- Electronic files created, sent, received, or stored on information resources owned, leased, administered, or otherwise under the custody and control of *Agency* are not private and may be accessed by *Agency IT* employees, for business reasons at any time without knowledge of the information resource user or owner.
- To manage systems and enforce security, the *Agency* may log, review, and otherwise utilize any information stored on or passing through its *IT* systems in accordance with the provisions and safeguards provided in the Texas Administrative Code 202, Information Resource Standards. For these same purposes, the *Agency* may also capture User activity such as IP addresses and web sites visited.
- A wide variety of third parties have entrusted their information to *Agency* for business purposes, and all workers at the *Agency* must do their best to safeguard the privacy and security of this information. The most important of these third parties is the individual customer; customer account data is accordingly confidential and access will be strictly limited based on business need for access.
- Users must report any weaknesses in *Agency* computer security, any incidents of possible misuse or violation of this agreement to the proper authorities. An internal email address, [Information Security](#), has been established within the *Agency* for reporting information security issues.
- Users must not attempt to access any data or programs contained on *Agency* systems for which they do not have authorization or explicit consent.

Support Information

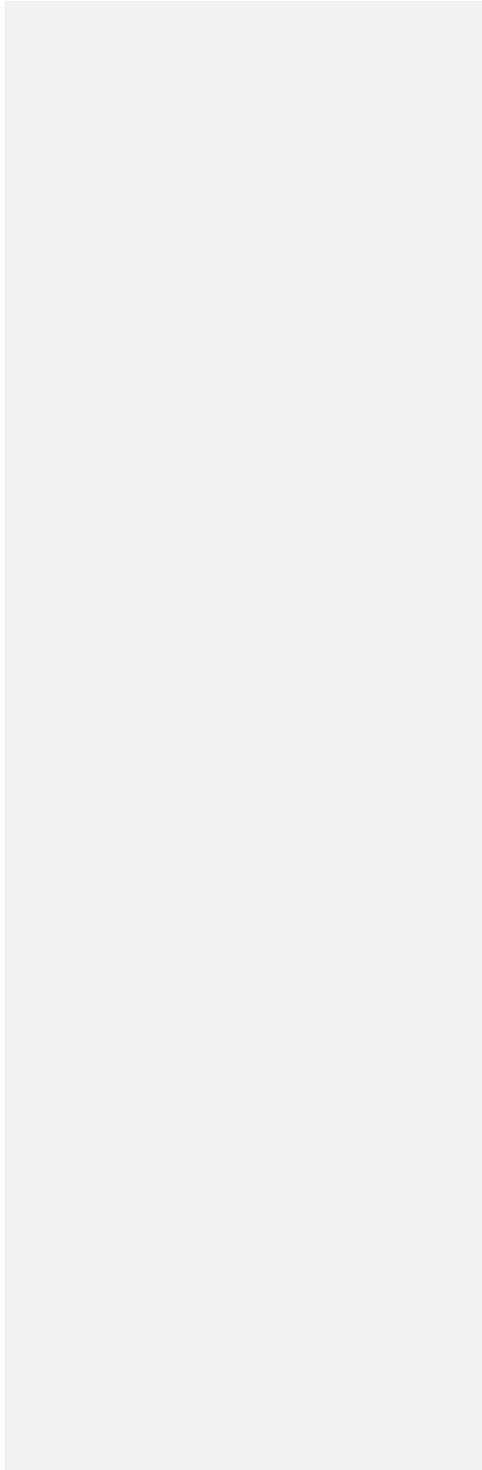
This Policy is supported by the Security Policy Standard.

Disciplinary Action

Violation of this policy may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of *Agency* information resources access privileges, as well as civil and criminal prosecution. Violations of this policy or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Policy of the Agency.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.1	Marlin Craig	02/17/18		Scott Brandt	03/05/18



SECURITY AWARENESS POLICY

Introduction

Understanding the importance of computer security and individual responsibilities and accountability for computer security are paramount to achieving organization security goals. This can be accomplished with a combination of general computer security awareness training and targeted, product specific training. The philosophy of protection and specific security instructions needs to be taught to, and re-enforced with, computer users. The security awareness and training information needs to be continuously upgraded and reinforced.

Purpose

The purpose of the Security Awareness Policy is to describe the requirements that will ensure each user of *Agency* information resources receives adequate training on information security awareness issues.

Security Awareness Policy

- All new users must complete an approved Security Awareness orientation prior to, or at least within 90 days of, being granted access to any *Agency* information resources.
- All users must sign an acknowledgement stating they have read and understand *Agency* requirements regarding computer security policies and procedures.
- All users (employees, consultants, contractors, temporaries, etc.) must be provided with sufficient training and supporting reference materials to allow them to properly protect *Agency* information resources.
- **IT** must prepare, maintain, and distribute one or more information security manuals that concisely describe *Agency* information security policies and procedures.
- **IT** must develop and maintain a communications process to be able to communicate new computer security program information, security bulletin information, and security items of interest as approved by the **ISO**.

Support Information

This Policy is supported by the Security Policy Standard.

Disciplinary Action

Violation of this policy may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of *Agency* information resources access privileges, as well as civil and criminal prosecution. Violations of this policy or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Policy of the Agency.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.1	Marlin Craig	02/10/18		Scott Brandt	03/05/18

SOFTWARE LICENSING POLICY

Introduction

End-user license agreements are used by software and other information technology companies to protect their valuable intellectual assets and to advise technology users of their rights and responsibilities under intellectual property and other applicable laws.

Purpose

The purpose of the Software Licensing Policy is to establish the rules for licensed software use on *Agency* information resources.

Software Licensing Policy

- The *Agency* provides a sufficient number of licensed copies of software such that workers can get their work done in an expedient and effective manner. Management must make appropriate arrangements with the involved vendor(s) for additional licensed copies if and when additional copies are needed for business activities.
- Third party copyrighted information or software, that the *Agency* does not have specific approval to store and/or use, must not be stored on *Agency* systems or networks. All software on *Agency* computers will be procured, maintained and installed by IT unless specific written approval is granted. System administrators may remove unauthorized material.
- Third party software in the possession of the *Agency* must not be copied unless such copying is consistent with relevant license agreements and prior management approval of such copying has been obtained, or copies are being made for contingency planning purposes.

Support Information

This Policy is supported by the Security Policy Standard.

Disciplinary Action

Violation of this policy may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of *Agency* information resources access privileges, as well as civil and criminal prosecution. Violations of this policy or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Policy of the Agency.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.1	Marlin Craig	02/20/17		Scott Brandt	03/05/18

EXCEPTION POLICY

Introduction

The *Agency* Information Security Policies provide the techniques and methodology to protect *Agency* information resource assets. While these Policies are technology independent they are more closely linked to the technology than the Policy Standards and are hence more likely to be impacted by changing technology, legislation, and business requirements. As with most policies there may be a need for exception.

Purpose

An exception is a method used to document variations from the rules

Exception Policy

In certain cases, compliance with specific policy requirements may not be immediately possible. Reasons include, but are not limited to, the following:

- Required commercial or other software in use is not currently able to support the required features;
- Legacy systems are in use which do not comply.
- Costs for reasonable compliance are disproportionate relative to the potential damage.

In such cases, a written explanation of the compliance issue must be developed and a plan for coming into compliance with the *Agency's* Information Security Policy in a reasonable amount of time. Explanations and plans should be submitted according to the process for approval:

The steps for permitting and documenting an exception are:

- A request for an exception is received by the **ISO** along with a business case for justifying the exception
- The **ISO** analyzes the request and the business case and determines if the exception should be accepted, denied, or if it requires more investigation
- If more investigation is required the **ISO** and **TMT** determine if there is a cost effective solution to the problem that does not require an exception
- If there is not an alternate cost effective solution, and the risk is minimal, the exception may be granted
- Each exception must be re-examined according to its assigned schedule. The schedule can vary from 3 months to 12 months depending on the nature of the exception

Any exception request that is rejected may be appealed to the **IRM**.

Support Information

This Policy is supported by the Security Policy Standard.

Support Information

Violation of this policy may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of *Agency* information resources access privileges, as well as civil and criminal prosecution. Violations of this policy or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Policy of the Agency.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.1	Marlin Craig	02/12/18		Scott Brandt	03/05/18

ADMINISTRATION/SPECIAL ACCESS POLICY

Introduction

Technical support staff, security administrators, system administrators and others may have special access account *privilege* requirements compared to typical or everyday users. The fact that these administrative and special access accounts have a higher level of access means that granting, controlling and monitoring these accounts is extremely important to an overall security program.

Purpose

The purpose of the *Agency* Administrative/Special Access Practice Standard is to establish the rules for the creation, use, monitoring, control and removal of accounts with special access privileges.

Administrative/ Special Access Policy

- *Agency* departments must submit to IT a list of administrative contacts for their systems that are connected to the *Agency* network.
- All users of Administrative/Special Access accounts must sign the *Agency* Information Security Acknowledgement and Nondisclosure Agreement before access is given to an account.
- All users of Administrative/Special access accounts must have account management instructions, documentation, training, and authorization.
- Each individual that uses Administrative/Special access accounts must refrain from abuse of privilege and must only do investigations under the direction of the ISO.
- Each individual that uses Administrative/Special access accounts must use the account privilege most appropriate with work being performed (i.e., user account vs. administrator account).
- Each account used for administrative/special access must meet the *Agency* Password Policy.
- The password for a shared administrator/special access account must change when an individual with the password leaves the department or *Agency*, or upon a change in the vendor personnel assigned to the *Agency* contract.
- In the case where a system has only one administrator there must be a password escrow procedure in place so that someone other than the administrator can gain access to the administrator account in an emergency situation.
- When Special Access accounts are needed for Internal or External Audit, software development, software installation, or other defined need, they:
 - ❖ Must be authorized by the ISO, must be created with a specific expiration date and must be removed when work is complete.

Support Information

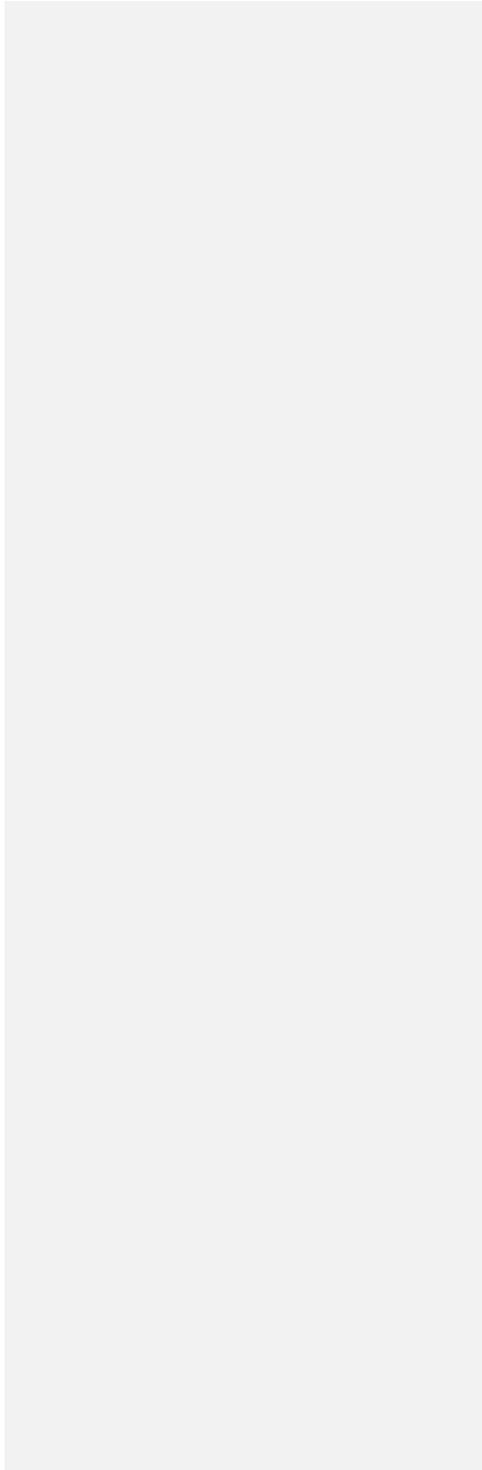
This Policy is supported by the Security Policy Standard.

Disciplinary Actions

Violation of this policy may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of *Agency* information resources access privileges, as well as civil and criminal prosecution. Violations of this policy or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Policy of the Agency.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.1	Marlin Craig	02/10/18		Scott Brandt	03/05/18



BACKUP/DIASTER RECOVERY POLICY

Introduction

Electronic backups are a business requirement to enable the recovery of data and applications in the case of events such as natural disasters, system disk drive failures, data entry errors, system operations errors or other data corruption.

Purpose

The purpose of the *Agency* Backup/DR Policy is to establish the rules for the backup and storage of electronic *Agency* information.

Backup/Disaster Recovery Policy

- SOS server operations have transitioned from in-house to infrastructure as a service (DIR Data Center Services) and application specific vendor managed services, the SOS IT organization is no longer responsible for recovery of server infrastructure. The frequency and extent of backups must be in accordance with the importance of the information and the acceptable risk as determined by the data owner (Information contained in SOS Information Technology Disaster Recovery Plan).
- The *DIR data Center services* backup and recovery process for each system must be documented and periodically reviewed by SOS.
- The vendor(s) providing offsite backup storage for *Agency* must be cleared to handle the highest level of information stored.
- Physical access controls implemented at offsite backup storage locations must meet or exceed the physical access controls of the source systems. Additionally backup media must be protected in accordance with the highest *Agency* sensitivity level of information stored.
- Backups must be periodically tested by *DIR data Center services* to ensure that they are recoverable.
- Procedures must be reviewed at least annually.

Support Information

This Policy is supported by the Security Policy Standard, and the SOS Information Technology Disaster Recovery Plan.

Support Information

Violation of this policy may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of *Agency* information resources access privileges, as well as civil and criminal prosecution. Violations of this policy or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Policy of the Agency.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.2	Marlin Craig	10/24/18		Scott Brandt	10/24/18

CHANGE MANAGEMENT POLICY

Introduction

The Information Technology infrastructure at the *Agency* is expanding and becoming more complex. There are more people dependent upon the network, more client machines, upgraded and expanded administrative systems, and more application programs. As the interdependency between Information Technology infrastructures grows, the need for a strong change management process is essential.

Managing these changes is a critical part of providing a robust and valuable Information Technology infrastructure.

Purpose

The purpose of the Change Management Policy is to manage changes in a rational and predictable manner so that staff and clients can plan accordingly. Changes require serious forethought, careful monitoring, and follow-up evaluation to reduce negative impact to the user community and to increase the value of information resource.

Definitions

Owner: The manager or agent responsible for the function which is supported by the resource, the individual upon whom responsibility rests for carrying out the program that uses the resources. The owner is responsible for establishing the controls that provide the security. The owner of a collection of information is the person responsible for the business results of that system or the use of the information. Where appropriate, ownership may be shared by managers of different departments.

Custodian: Guardian or caretaker; the holder of data, the agent charged with implementing the controls specified by the owner. The custodian is responsible for the processing and storage of information. For mainframe applications Information Technology is the custodian; for micro and mini applications the owner or user may retain custodial responsibilities. The custodian is normally a provider of services.

Change Management: The process of controlling modifications to hardware, software, firmware, and documentation to ensure that information is protected against improper modification before, during, and after system implementation.

Change:

- any implementation of new functionality
- any interruption of service
- any repair of existing functionality
- any removal of existing functionality

Scheduled Change: Formal notification received, reviewed, and approved by the review process in advance of the change being made.

Unscheduled Change: Failure to present notification to the formal process in advance of the change being made. Unscheduled changes will only be acceptable in the event of a system failure, the discovery of security vulnerability or other emergency.

Emergency Change: When an unauthorized immediate response to imminent critical system failure is needed to prevent widespread service disruption.

Change Management Policy

- Every change to an *Agency* IT resource such as: operating systems, computing hardware, networks, and

applications is subject to the Change Management Policy and must follow the Change Management Procedures.

- All changes affecting computing environmental facilities (e.g., air-conditioning, water, heat, plumbing, electricity, and alarms) should be reported to or coordinated with the leader of the change management process.
- The **TMT** Committee will meet regularly to review change requests and to ensure that change reviews and communications are being satisfactorily performed.
- A formal written change notification must be submitted for all changes, both scheduled and unscheduled.
- All scheduled change notifications must be submitted in accordance with change management procedures so there is time to review the request, determine and review potential failures, and make the decision to allow or delay the request.
- The appointed leader of the **IRM** may deny a scheduled or unscheduled change for reasons including, but not limited to, inadequate planning, inadequate back out plans, the timing of the change will negatively impact a key business process such as year end accounting, or if adequate resources cannot be readily available.
- A Change Review shall be completed for each change, whether scheduled or unscheduled, and whether successful or not.
- A Change Management Log must be maintained for all changes. The log must contain, but is not limited to:

- ❖ Date of submission and date of change
- ❖ Owner and custodian contact information
- ❖ Nature of the change
- ❖ Indication of success or failure
- ❖ Instructions for making the change, and rolling back the change

All **Agency** information systems must comply with an **IT** change management process that meets the standards outlined above.

Support Information

This Policy is supported by the Security Policy Standard.

Disciplinary Action

Violation of this policy may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of **Agency** information resources access privileges, as well as civil and criminal prosecution. Violations of this policy or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Policy of the Agency.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.1	Marlin Craig	02/20/18		Scott Brandt	03/05/18

INCIDENT MANAGEMENT POLICY

Introduction

The number of computer security incidents and the resulting cost of business disruption and service restoration continue to escalate. Implementing solid security policies, blocking unnecessary access to networks and computers, improving user security awareness, and early detection and mitigation of security incidents are some the actions that can be taken to reduce the risk and drive down the cost of security incidents.

Purpose

This document describes the requirements for dealing with computer security incidents. Security incidents include, but are not limited to: virus, worm, and Trojan horse detection, unauthorized use of computer accounts and computer systems, as well as complaints of improper use of information resources, as outlined in the Email Policy and the Acceptable Use Policy.

Definitions

Computer Incident Response Team (CIRT): Personnel responsible for coordinating the response to computer security incidents in an organization

Virus: A program that attaches itself to an executable file or vulnerable application and delivers a payload that ranges from annoying to extremely destructive. A file virus executes when an infected file is accessed. A macro virus infects the executable code embedded in Microsoft Office programs that allow users to generate macros.

Worm: A program that makes copies of itself elsewhere in a computing system. These copies may be created on the same computer or may be sent over networks to other computers. The first use of the term described a program that copied itself benignly around a network using otherwise unused resources on networked machines to perform distributed computation. Some worms are security threats, using networks to spread themselves against the wishes of the system owners, and disrupting networks by overloading them. A worm is similar to a virus in that it makes copies of itself, but different in that it need not attach to particular files or sectors at all.

Trojan Horse: Destructive programs—usually viruses or worms—that are hidden in an attractive or innocent-looking piece of software, such as a game or graphics program. Victims may receive a Trojan horse program by e-mail or on a diskette, often from another unknowing victim, or may be urged to download a file from a Web site or bulletin board.

Security Incident: In information operations, an assessed event of attempted entry, unauthorized entry, or an information attack on an automated information system. It includes unauthorized probing and browsing; disruption or denial of service; altered or destroyed input, processing, storage, or output of information; or changes to information system hardware, firmware, or software characteristics with or without the users' knowledge, instruction, or intent.

Vendor: someone who exchanges goods or services for money.

Incident Management Practice Standard Policy

- **Agency** CIRT members have pre-defined roles and responsibilities which can take priority over normal duties.

- Whenever a security incident, such as a virus, worm, hoax email, discovery of hacking tools, altered data, etc. is suspected or confirmed, the appropriate Incident Management procedures must be followed.
- The **ISO** is responsible for notifying the **IRM** within 24 hours of verifying incident and notifying DIR-NSOC, and the Deputy Secretary of State within 48 hours of verifying incident.
- The **ISO** is responsible for notifying the CIRT and initiating the appropriate incident management action including restoration as defined in the Incident Management Procedures.
- The **ISO** is responsible for determining the physical and electronic evidence to be gathered as part of the Incident Investigation.
- The appropriate technical resources from the CIRT are responsible for monitoring that any damage from a security incident is repaired or mitigated and that the vulnerability is eliminated or minimized where possible.
- The **ISO**, working with the **IRM**, will determine if a widespread *Agency* communication is required, the content of the communication, and how best to distribute the communication.
- The appropriate technical resources from the CIRT are responsible for communicating new issues or vulnerabilities to the system vendor and working with the vendor to eliminate or mitigate the vulnerability.
- The **ISO** is responsible for initiating, completing, and documenting the incident investigation with assistance from the CIRT.
- The *Agency* **ISO** is responsible for reporting the incident to the:

- ❖ **IRM**
- ❖ Department of Information Resources as outlined in TAC 202
- ❖ Local, state or federal law officials as required by applicable statutes and/or regulations

- The **ISO** is responsible for coordinating communications with outside organizations and law enforcement.
- In the case where law enforcement is not involved, the **ISO** will recommend disciplinary actions, if appropriate, to the **IRM**.
- In the case where law enforcement is involved, the **ISO** will act as the liaison between law enforcement and *Agency*.

Support Information

This Policy is supported by the Security Policy Standard.

Disciplinary Action

Violation of this policy may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of *Agency* information resources access privileges, as well as civil and criminal prosecution. Violations of this policy or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Policy of the Agency.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.2	Marlin Craig	10/24/18		Scott Brandt	10/24/18

INTRUSION DETECTION POLICY

Introduction

Intrusion detection plays an important role in implementing and enforcing an organizational security policy. As information technologies grow in complexity, effective security systems must evolve. With the proliferation of the number of vulnerability points introduced by the use of distributed systems some type of assurance is needed that the systems and network are secure. Intrusion detection systems can provide part of that assurance.

Purpose

Intrusion detection provides two important functions in protecting information resources:

- Feedback: information as to the effectiveness of other components of the security system. If a robust and effective intrusion detection system is in place, the lack of detected intrusions is an indication that other defenses are working.
- Trigger: a mechanism that determines when to activate planned responses to an intrusion incident.

Intrusion Detection Policy

- Intruder detection must be implemented for all servers containing data classified as high risk.
- Operating system and application software logging processes should be enabled on all critical server systems. Where possible, alarm and alert functions, as well as logging and monitoring systems should be enabled.
- Server, firewall, and critical system logs should be reviewed frequently. Where possible, automated review should be enabled and alerts should be transmitted to the administrator when a serious security intrusion is detected.
- Intrusion tools should be installed where appropriate and checked on a regular basis.

Support Information

This Policy is supported by the Security Policy Standard.

Disciplinary Action

Violation of this policy may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of *Agency* information resources access privileges, as well as civil and criminal prosecution. Violations of this policy or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Policy of the Agency.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.1	Marlin Craig	02/15/18		Scott Brandt	03/05/18

NETWORK CONFIGURATION POLICY

Introduction

The *Agency* network infrastructure is provided as a central utility for all users of *Agency* information resources. It is important that the infrastructure, which includes cabling and the associated equipment such as routers and switches, continues to develop with sufficient flexibility to meet user demands while at the same time remaining capable of exploiting anticipated developments in high speed networking technology to allow the future provision of enhanced user services.

Purpose

The purpose of the *Agency* Network Configuration Security Policy is to establish the rules for the maintenance, expansion and use of the network infrastructure. These rules are necessary to preserve the integrity, availability, and confidentiality of *Agency* information.

Network Configuration Policy

- *Agency* Information Technology (IT) owns and is responsible for the *Agency* network infrastructure and will continue to manage further developments and enhancements to this infrastructure.
- To provide a consistent *Agency* network infrastructure capable of exploiting new networking developments, all cabling must be installed by *Agency* IT or an approved contractor.
- All network connected equipment must be configured to a specification approved by *Agency* IT.
- All hardware connected to the *Agency* network is subject to *Agency* IT management and monitoring standards.
- Changes to the configuration of active network management devices must not be made without the approval of *Agency* IT.
- The *Agency* network infrastructure supports a well-defined set of approved networking protocols. Any use of non-sanctioned protocols must be approved by *Agency* IT.
- The networking addresses for the supported protocols are allocated, registered and managed centrally by *Agency* IT.
- All connections of the network infrastructure to external third party networks are the responsibility of *Agency* IT. This includes connections to external telephone networks.
- *Agency* IT Firewalls must be installed and configured following the *Agency* Firewall Implementation Standard documentation.
- Firewall rules will be reviewed annually.
- The use of departmental firewalls is not permitted without the written authorization from *Agency* IT.
- Users must not extend or re-transmit network services in any way. This means you must not install a router, switch, hub, or wireless access point to the *Agency* network without *Agency* IT approval.
- Users must not install network hardware or software that provides network services without *Agency* IT approval.
- Users are not permitted to alter network hardware in any way.

Support Information

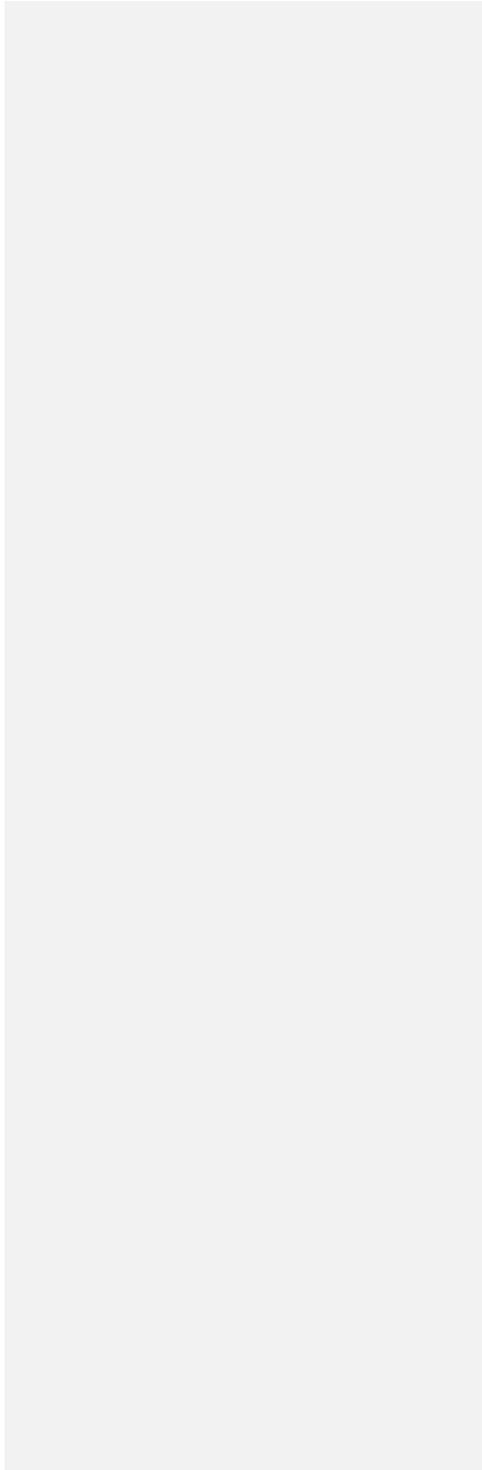
This Policy is supported by the Security Policy Standard.

Disciplinary Action

Violation of this policy may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of *Agency* information resources access privileges, as well as civil and criminal prosecution. Violations of this policy or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Policy of the Agency.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.1	Marlin Craig	02/02/18		Scott Brandt	03/05/18



PHYSICAL ACCESS POLICY

Introduction

Technical support staff, security administrators, system administrators, and others may have Information Technology physical facility access requirements as part of their function. The granting, controlling, and monitoring of the physical access to Information Technology facilities is extremely important to an overall security program.

Purpose

The purpose of the *Agency* Physical Access Policy is to establish the rules for the granting, control, monitoring, and removal of physical access to Information Technology facilities.

Physical Access Policy

- All physical security systems must comply with all applicable regulations such as, but not limited to, building codes and fire prevention codes.
- Physical access to all Information Technology restricted facilities must be documented and managed.
- All **IT** facilities must be physically protected in proportion to the criticality or importance of their function at the *Agency*.
- Access to **IT** facilities must be granted only to *Agency* support personnel, and contractors, whose job responsibilities require access to that facility.
- The process for granting card and/or key access to **IT** facilities must include the approval of the person responsible for the facility.
- Each individual that is granted access rights to an **IT** facility must receive emergency procedures training for the facility and must sign the appropriate access and non-disclosure agreements.
- Requests for access must come from the applicable *Agency* data/system owner.
- Access cards and/or keys must not be shared or loaned to others.
- Access cards and/or keys that are no longer required must be returned to the person responsible for the Information Technology facility. Cards must not be reallocated to another individual bypassing the return process.
- Lost or stolen access cards and/or keys must be reported to the person responsible for the **IT** facility immediately.
- Cards and/or keys must not have identifying information other than a return mail address.
- All **IT** facilities that allow access to visitors will track visitor access with a sign in/out log.
- A service charge may be assessed for access cards and/or keys that are lost, stolen or are not returned.
- Card access records and visitor logs for **IT** facilities must be kept for routine review based upon the criticality of the information resources being protected. The person responsible for the **IT** facility must remove the card and/or key access rights of individuals that change roles within *Agency* or are separated from their relationship with *Agency*.
- Visitors must be escorted in card access controlled areas of **IT** facilities.
- The person responsible for the **IT** facility shall review access records and visitor logs for the facility on a periodic basis and investigate any unusual access.

- The person responsible for the IT facility must review card and/or key access rights for the facility on annual basis and remove access for individuals that no longer require access.
- Signage for restricted access rooms and locations must be practical, yet minimal discernible evidence of the importance of the location should be displayed.

Support Information

This Policy is supported by the Security Policy Standard.

Disciplinary Action

Violation of this policy may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of *Agency* information resources access privileges, as well as civil and criminal prosecution. Violations of this policy or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Policy of the Agency.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.1	Marlin Craig	02/20/18		Scott Brandt	03/05/18

SYSTEM DEVELOPMENT POLICY

Introduction

The development of new systems, applications or major enhancements to existing systems is often the result of significant changes made to the processes they support. Ideally, the efforts to simplify business processes will be done by the functional office in conjunction with the technical staff, so that current technologies can be considered as the processes are reviewed. Ultimately, the most important criteria for development is to create changes that are best for the *Agency* as a whole.

Purpose

The purpose of the System Development Policy is to describe the requirements for developing and/or implementing new software within the *Agency*.

Definitions

System Development Life Cycle (SDLC): a set of procedures to guide the development of production application software and data items. A typical SDLC includes design, development, maintenance, quality assurance and acceptance testing.

Owner: The manager or agent responsible for the function which is supported by the resource, the individual upon whom responsibility rests for carrying out the program that uses the resources. The owner is responsible for establishing the controls that provide the security. The owner of a collection of information is the person responsible for the business results of that system or use of the information. Where appropriate, ownership may be shared by managers of different departments

Custodian: Guardian or caretaker; the holder of data, the agent charged with implementing the controls specified by the owner. The custodian is responsible for the processing and storage of information. For mainframe applications, Information Services is the custodian; for micro and mini applications, the owner or user may retain custodial responsibilities. The custodian is normally a provider of services.

User: Has the responsibility to (1) use the resource only for the purpose specified by the owner, (2) comply with controls established by the owner, and (3) prevent disclosure of confidential or sensitive information. The user is any person who has been authorized to read, enter, or update information by the owner of the information. The user is the single most effective control for providing adequate security.

Production System: The hardware, software, physical, procedural, and organizational issues that need to be considered when addressing the security of an application, group of applications, organizations, or group of organizations.

System Development Policy

- Information Technology (IT) is responsible for developing, maintaining, and participating in a System Development Life Cycle (SDLC) for *Agency* system development projects. All software developed in-house which runs on production systems should be developed according to the SDLC. At a minimum, this plan should address the areas of preliminary analysis or feasibility study; risk identification and mitigation;

systems analysis; general design; security design, detail design; development; quality assurance, and acceptance testing; implementation; and post-implementation maintenance and review. This methodology ensures that the software will be adequately documented and tested before it is used for critical *Agency* information.

- All production systems must have designated Owners and Custodians for the critical information they process. **IT** must perform periodic formal risk assessments of production systems to determine whether the controls employed are adequate, and meet state requirements.
- All production systems must have an access control system to restrict who can access the system as well as restrict the privileges available to these users. A designated access control administrator (who is not a regular user on the system in question) must be assigned for all production systems.
- Where resources permit, there should be a separation between the production, development, and test environments. This will ensure that security is rigorously maintained for the production system, while the development and test environments can maximize productivity with fewer security restrictions. Migration of code between SDLC environments must comply with the Change Management Policy. All production software testing must utilize sanitized information.
- All application-program-based access paths other than the formal user access paths must be deleted or disabled before software is moved into production.

Support Information

This Policy is supported by the Security Policy Standard.

Disciplinary Action

Violation of this policy may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of *Agency* information resources access privileges, as well as civil and criminal prosecution. Violations of this policy or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Policy of the Agency.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.2	Marlin Craig	10/24/18		Scott Brandt	10/24/18

SECURITY MONITORING POLICY

Introduction

Security Monitoring is a method used to confirm that the security practices and controls in place are being adhered to and are effective. Monitoring consists of activities such as but not limited to the review of:

- Automated intrusion detection system logs
- Firewall logs
- IPS logs
- Anti-virus logs
- User account logs
- Network scanning logs
- Application logs
- Data backup recovery logs
- Help desk logs
- Other log and error files.

Purpose

The purpose of the Security Monitoring Policy is to ensure that Information Technology security controls are in place, are effective, and are not being bypassed. One of the benefits of security monitoring is the early identification of wrongdoing or new security vulnerabilities. This early identification can help to block the wrongdoing or vulnerability before harm can be done, or at least to minimize the potential impact. Other benefits include Audit Compliance, Service Level Monitoring, Performance Measurement, Limitation of Liability, and Capacity Planning.

Security Monitoring Policy

- Automated tools will be used by the *Agency IT* to provide real time notification of detected wrongdoing and vulnerability exploitation. Where possible a security baseline will be developed and the tools will report exceptions. These tools will be deployed to monitor:

- ❖ Internet traffic
- ❖ Electronic mail traffic
- ❖ LAN traffic, protocols, and device inventory
- ❖ Operating system security parameters

- The following files will be checked for signs of wrongdoing and vulnerability exploitation at a frequency determined by risk:

- ❖ Automated intrusion detection system logs
- ❖ Firewall logs
- ❖ User account logs
- ❖ Network scanning logs
- ❖ System error logs
- ❖ Application logs
- ❖ Data backup and recovery logs
- ❖ Help desk trouble tickets

- The following checks will be performed at least quarterly by assigned individuals:

- ❖ Password strength
- ❖ Unauthorized network devices
- ❖ Unauthorized personal web servers
- ❖ Unsecured sharing of devices
- ❖ Operating System and Software Licenses

Any security issues discovered will be reported for follow-up investigation. An internal email address, [Information Security](#), has been established within the *Agency* for reporting information security issues.

Support Information

This Policy is supported by the Security Policy Standard.

Disciplinary Action

Violation of this policy may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of *Agency* information resources access privileges, as well as civil and criminal prosecution. Violations of this policy or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Policy of the Agency.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.1	Marlin Craig	02/12/18		Scott Brandt	03/05/18

SYSTEM SECURITY POLICY

Introduction

Servers are depended upon to deliver data in a secure, reliable fashion. There must be assurance that data integrity, confidentiality and availability are maintained. One of the required steps to attain this assurance is to ensure that the servers are installed and maintained in a manner that prevents unauthorized access, unauthorized use, and disruptions in service.

Purpose

The purpose of the *Agency* System Security Policy document is to describe the requirements for installing a new system in a secure fashion and maintaining the security of the server and application software.

System Security Policy

All systems introduced on the *Agency* network should be made secure before placing them into production. This is known as “hardening” the systems. This process should be a combination of vendor recommendations, and industry best practices and procedures as deemed appropriate.

- Installing the operating system from an IT approved source.
- All systems connected to the *Agency* network should have a vendor supported version of the operating system installed.
- All systems connected to the *Agency* network should be current with security patches, hot fixes or updates for operating systems and applications. Security patches, hot fixes or updates must be applied in a timely manner, as approved by the TMT, to protect *Agency* information resources.
- Setting security parameters, file protections and enabling audit logging.
- Warning banners must be established, as appropriate, on all system access points. The approved *Agency* warning banner is included in Appendix A of this policy.
- All unnecessary services should be disabled.
- Systems in the final stages of hardening may be placed on the *Agency* network in an isolated segment such as a segmented lab environment to minimize exposure.
- Systems should be harden according to a benchmark standard like CIS when possible.
- Vulnerability scans or penetration tests must be performed on all Internet-facing applications and systems before placement into production. At a minimum, quarterly audits must be conducted to re-evaluate the risk potential of applications and systems.
- System integrity checks of server systems housing high risk *Agency* data should be performed.

Support Information

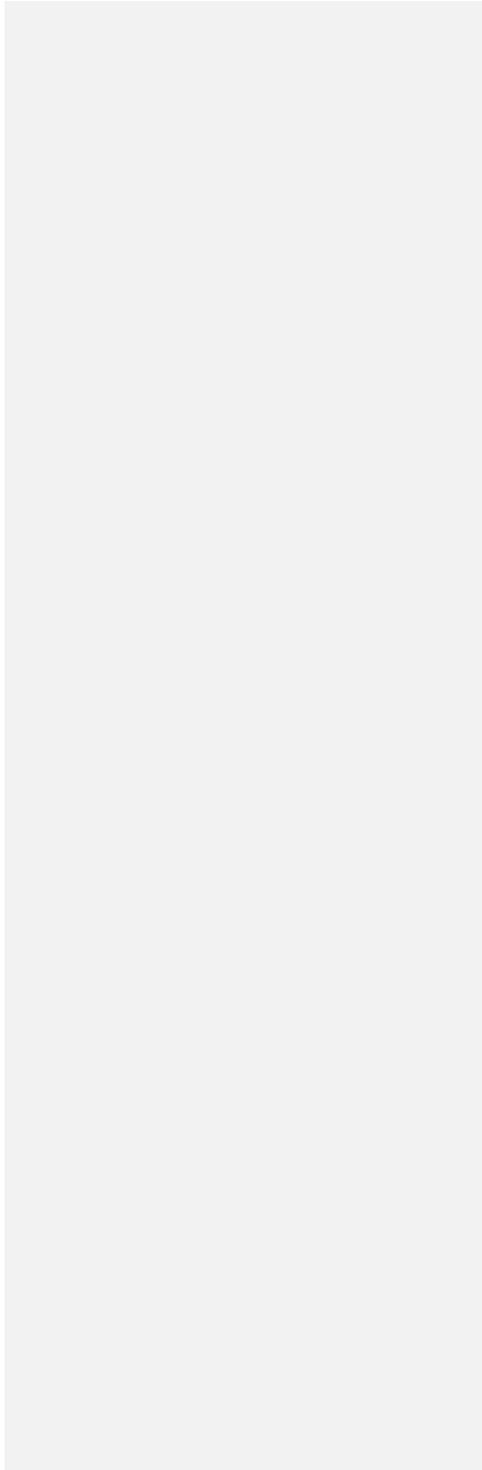
This Policy is supported by the Security Policy Standard.

Disciplinary Action

Violation of this policy may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of *Agency* information resources access privileges, as well as civil and criminal prosecution. Violations of this policy or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Policy of the Agency.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.1	Marlin Craig	02/12/18		Scott Brandt	03/05/18



Appendix A to the System Security Policy

Approved Agency Warning Banner

***** WARNING! *****

Unauthorized use of this system is prohibited and may be subject to criminal prosecution. The System Administrator may monitor any activity or communication on the system and retrieve any information stored within the system. By accessing this system, you are consenting to such monitoring and information retrieval. You should have no expectation of privacy as to any communication on or information stored within this system except as explicitly stated in officially approved system privacy policies. Unauthorized or improper use of this system is a violation of law and may be prosecuted resulting in criminal, civil, and/or administrative penalties.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.1	Marlin Craig	02/20/18		Scott Brandt	03/05/18

VENDOR ACCESS POLICY

Introduction

Vendors play an important role in the support of hardware and software management, and operations for customers. Vendors can remotely view, copy and modify data and audit logs, they correct software and operating systems problems; they can monitor and fine tune system performance; they can monitor hardware performance and errors; they can modify environmental systems, and reset alarm thresholds. Setting limits and controls on what can be seen, copied, modified, and controlled by vendors will eliminate or reduce the risk of loss of revenue, liability, loss of trust, and embarrassment to the *Agency*.

Purpose

The purpose of the *Agency* Vendor Access Policy is to establish the rules for vendor access to *Agency* information resources and support services (A/C, UPS, PDU, fire suppression, etc.), vendor responsibilities, and the protection of *Agency* information.

Vendor Access Policy

- Vendors must comply with all applicable *Agency* policies, practice standards and agreements, including, but not limited to:
 - ❖ Safety Policies
 - ❖ Privacy Policies
 - ❖ Security Policies
 - ❖ Auditing Policies
 - ❖ Software Licensing Policies
 - ❖ Acceptable Use Policies
- Vendor agreements and contracts must specify:
 - ❖ The *Agency* information the vendor should have access to
 - ❖ How *Agency* information is to be protected by the vendor
 - ❖ Acceptable methods for the return, destruction or disposal of *Agency* information in the vendor's possession at the end of the contract
 - ❖ The Vendor must only use *Agency* information and information resources for the purpose of the business agreement
 - ❖ Any other *Agency* information acquired by the vendor in the course of the contract cannot be used for the vendor's own purposes or divulged to others
- The *Agency* will provide an IT point of contact for the Vendor. The point of contact will work with the Vendor to make certain the Vendor is in compliance with these policies.
- Each vendor must provide the *Agency* with a list of all employees working on the contract. The list must be updated and provided to the *Agency* within 24 hours of staff changes.
- Each on-site vendor employee must acquire an *Agency* identification badge that will be displayed at all times while on *Agency* premises. The badge must be returned to the *Agency* when the employee leaves the contract or at the end of the contract.
- Each vendor employee with access to *Agency* sensitive information must be cleared to handle that information.
- Vendor personnel must report all security incidents directly to the ISO or agency security personnel.

- If vendor management is involved in *Agency* security incident management, the responsibilities and details must be specified in the contract.
- Vendor must follow all applicable *Agency* change control processes and procedures.
- Regular work hours and duties will be defined in the contract. Work outside of defined parameters must be approved in writing by appropriate *Agency* management.

Support Information

This Policy is supported by the Security Policy Standard.

Disciplinary Action

Violation of this policy may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of *Agency* information resources access privileges, as well as civil and criminal prosecution. Violations of this policy or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Policy of the Agency.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.1	Marlin Craig	03/01/18		Scott Brandt	03/05/18

COMPUTER SECURITY BREACH NOTIFICATION POLICY

Introduction

The *Agency* shall provide timely and appropriate notice to affected individuals when there is reasonable belief that a breach in the security of private information or highly sensitive information has occurred. Please review the Data Classification Policy for definitions and information classifications. A breach in security is defined as an unauthorized acquisition of information, and/or as defined by applicable local, state, or federal laws or regulations.

Purpose

Attacks on *Agency* resources are infractions of the Acceptable Use Policy constituting misuse, or they may be vandalism or other criminal behavior. Reporting information security breaches occurring on *Agency* systems and/or on *Agency* networks to appropriate authorities is a requirement of all persons affiliated with the *Agency* in any capacity.

Computer Security Breach Notification Policy

Suspected or confirmed information security breaches must be reported to the **Agency Information Security Officer (ISO)**. The ISO may be contacted via email at [Information Security](#) or phone (512) 463-0505.

The ISO will investigate the report, and if a security breach of private and/or highly sensitive information has occurred, will inform the Department of Information Resources (DIR), Agency Directors, Executive Management and/or law enforcement, as appropriate.

In the event that a public notification of the security breach may be warranted, the ISO will consult with the **Information Resources Manager (IRM)**, appropriate Agency Directors, Executive Management and General Counsel to develop the response and make the final determination if a public notification of the event is warranted.

Procedures:

The entity responsible for support of the system or network under attack is expected to:

- A. Report the attack to the **ISO**, and follow the SOS Incident Response Policy.

Internal Notifications

The *Agency ISO* will report computer security breaches to the appropriate personnel in a timely manner. The **ISO** will consult with the **IRM**, and decide if the Critical Incident Response Team (CIRT) must be convened to determine a response strategy, or if an alternate group is appropriate for the response. This determination may be made prior to completion of the investigation of the security breach.

Determination of External Notification

To determine if unencrypted private or highly sensitive information has been acquired, or is reasonably believed to have been acquired by an unauthorized person, the following should be considered:

- A. Physical possession (lost or stolen device?)

- B. Credible evidence the information was copied/removed
- C. Length of time between intrusion and detection
- D. Purpose of the intrusion was acquisition of information
- E. Credible evidence the information was in a useable format
- F. Results of a forensic analysis of the system
- G. Ability to reach the affected individuals
- H. Applicable *Agency* policy, and/or local, state, or federal laws or regulations

External Notification

If it is determined that an external notification to the affected individuals is warranted, the following procedures will apply:

- A. Written notice will be provided to the affected individuals using US Mail, unless the cost is excessive or insufficient contact information exists. The letter will be developed by the department responsible for the system experiencing the breach, and approved by General Counsel and/or others as appropriate. The excessiveness of cost consideration will be the decision of the Executive Management, General Counsel, and others as appropriate.
- B. If written notice to the affected individuals is not feasible, the following methods should be considered for providing notice:
 - 1. Personal e-mail notices (provided addresses are available), developed by the department responsible for the system experiencing the breach, and approved by the Executive Management, General Counsel, and others as appropriate.
 - 2. A press release to media, to be written department responsible for the system experiencing the breach, and approved by Media Relations, Executive Management, General Counsel, and others as appropriate.
 - 3. An informational web site, developed by the department responsible for the system experiencing the breach, and approved by the Executive Management, General Counsel, and others as appropriate, with a conspicuous link in the *Agency* Home Page News area.
 - 4. Any other method of notification as deemed acceptable by Executive Management, General Counsel, and others as appropriate.
- C. The responsibility of expenses associated with external notification will be determined and approved by the Executive Management, General Counsel, and others as appropriate.

Definitions:

Private Information

If the information acquired includes a name (first and last name or first initial and last name) in combination with any of the following, and the information was not in an encrypted format, a public notification may be warranted:

- A. Social security number
- B. Driver’s license Number
- C. Bank Account, Credit, or Debit Card Account number with security, access, PIN, or password that would permit access to the account
- D. Any information classified as Confidential or High Risk in the *Agency* Data Classification Policy. Any information considered as private or sensitive by applicable *Agency* policy, and/or local, state, or federal laws or regulations.

Personal information that is publicly and lawfully available to the general public, such as address, phone number, and email address are not considered private information for the purposes of this policy.

Highly Sensitive Information

If the information acquired is of a very sensitive, confidential, or proprietary nature, the security breach will be investigated and will determine if a public notification is warranted. Examples of highly sensitive information include but are not limited to:

- A. Name, Address, with Date of Birth
- B. Information subject to contractual confidentiality provisions
- C. Security codes, combinations, or passwords

Support Information

This Policy is supported by the Security Policy Standard.

Disciplinary Action

Violation of this policy may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of *Agency* information resources access privileges, as well as civil and criminal prosecution. Violations of this policy or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Policy of the Agency.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.2	Marlin Craig	01/13/18		Scott Brandt	03/05/2018