ESBD – Package 10
RFO: 306-14-8485
Addenda #3

1. Regarding the security policies, is there a plan to still provide and require review and signature? Where do you want it in the response, which Tab?
   Forgive me, this was missed when the original documents were posted. Please find it on the next pages of this package. Include the signed copies in Tab 14 of the Offer response.

   Please sign to acknowledge this addendum. Place acknowledgement in Tab 12.

Signature Date

Printed or Typed Name of the above

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. These security policies are established to achieve the following:

- ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources.
- establish prudent and acceptable practices regarding the use of information resources.
- educate individuals who may use information resources on their responsibilities associated with such use.

Audience

The policies apply equally to all individuals granted access privileges to any Texas State Library and Archives Commission (TSLAC) Information Resources.

This document serves as a summary of the TSLAC security policies that guide a vendor's use of TSLAC information resources. Vendors must read the summary and acknowledge that they understand and will comply with this summary before they are given access to TSLAC resources.

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 TSLAC are the property of TSLAC. Amended (04-24-2012) – The exception to this statement is proprietary source code.

Privacy

Electronic files created, sent, received, or stored on Information Resources owned, leased, administered, or otherwise under the custody and control of TSLAC are not private and may be accessed by TSLAC IRT 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 1 TAC 202, Information Security Standards. Amended (04-24-2012) – The exception to this statement is proprietary source code.

Review

These policies are reviewed by the TSLAC Information Resources Manager (IRM) or a designated representative at least annually or when a change to the policies is needed.

A Guide to the Security Policies

There are eleven (11) security policies that relate to a vendor's use of TSLAC information resources. These policies are presented here.

Name of Policy	Brief Description	Page
Acceptable Use	Computer users responsibilities for IT resources	3
Internet Use	Acceptable practices regarding use of the Internet	4
IRT Privacy	Privacy expectations when using TSLAC IT resources	5
Network Access	Rules for accessing the TSLAC network	5
Password	Rules for creating and managing user authentication	5
Portable Computing	Rules for using Portable devices to access the network	6
Security Training	Rules for training computer users on security issues	7
Software Licensing	Rules for using software at TSLAC	7
Computer Virus Detection	Rules for handling computer viruses	7
Virtual Private Network	Rules for using remote access into the network	7
Data Management	Responsibilities for managing TSLAC data resources	9

Information Resources Acceptable Use Policy

- The purpose of the Acceptable Use Policy is to establish the rules computer users must follow when using TSLAC information resources.
- Users must not attempt to access any data or programs for which they do not have authorization.
- Users must not: harass, threaten or abuse others; degrade the performance of IT Resources; deprive an authorized user access to a TSLAC resource; obtain resources beyond those allocated; circumvent TSLAC computer security measures.
- TSLAC Information Resources must not be used for personal benefit.
- Users must not intentionally access, create, store or transmit material which TSLAC may deem to be offensive, indecent or obscene.
- Internet access on a TSLAC-owned, home based, computer adheres to the same policies that apply to use from within TSLAC facilities. Non-employees must not access TSLAC computer systems except vendors approved for this access.
- Users must not otherwise engage in acts against the aims and purposes of TSLAC as specified in its governing documents or in rules, regulations and procedures adopted from time to time.

Incidental Use

As a convenience to TSLAC computer users, incidental use of Information Resources is permitted. The following restrictions apply:

- Incidental personal use of IT resources is restricted to TSLAC approved users and does not extend to non-employees.
- Incidental use must not result in direct costs to TSLAC.
- Incidental use must not interfere with the normal performance of an employee's work duties.
- No files may be sent or received that may cause legal action against, or embarrassment to, TSLAC.
- Storage of personal email messages, voice messages files and documents within TSLAC's Information Resources must be nominal.
- All messages and documents – including personal messages and documents – on TSLAC Resources are owned by TSLAC, may be subject to open records requests, and may be accessed in accordance with this policy. Amended (04-24-2012) – The exception to this statement is proprietary source code.

Internet Usage Policy

- The purpose of the TSLAC Internet Usage Policy is to establish the rules for the use of TSLAC Internet.
- Software for browsing the Internet is provided to authorized users for business and research use only.
- All files downloaded from the Internet must be scanned for viruses using the approved IRT distributed software suite and current virus detection software.
- All sites accessed must comply with the TSLAC Acceptable Use Policy.
- All user activity on TSLAC Resources is subject to logging and review.
- Content on all TSLAC Web sites must comply with the TSLAC Acceptable Use Policy.
- No offensive or harassing material may be made available via TSLAC Web sites.
- TSLAC Internet access may not be used for personal gain.
- All sensitive and confidential TSLAC material transmitted over external networks must be encrypted.
- Electronic files are subject to the same records retention rules that apply to other TSLAC documents.

Incidental Use

- Incidental personal use of Internet access is restricted to TSLAC approved users.
- Incidental use must not result in direct costs to TSLAC.
- Incidental use must not interfere with the normal performance of an employee's work duties.
- No files or documents may be sent or received that may cause legal liability for, or embarrassment to, TSLAC.
- Storage of personal files and documents within TSLAC's Information Resources should be nominal.
- All files and documents – including personal files and documents – are owned by TSLAC, may be subject to open records requests, and may be accessed in accordance with this policy. Amended (04-24-2012) – The exception to this statement is proprietary source code.

IRT Privacy Policy

- The purpose of the TSLAC Information Services Privacy Policy is to clearly communicate the TSLAC Information Services Privacy expectations to Information Resources users
- Electronic files created, sent, received, or stored on IR owned, leased, administered, or otherwise under the custody and control of TSLAC are not private and may be accessed by TSLAC IRT employees at any time without knowledge of the IR user or owner. Amended (04-24-2012) – The exception to this statement is proprietary source code.
- TSLAC may log, review, and otherwise utilize any information stored on or passing through its IR systems in accordance with the provisions and safeguards provided in the Texas Administrative Code Section 1 TAC 202, Information Security Standards. For these same purposes, TSLAC may also capture user activity such as web sites visited.
- A wide variety of third parties have entrusted their information to TSLAC for business purposes, and all workers and all information resources users at TSLAC 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.

Network Access Policy

- The purpose of the TSLAC Network Access Policy is to establish the rules for the access and use of TSLAC network infrastructure.
- Users are permitted to use only those network addresses issued to them by TSLAC IRT.
- 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 TSLAC network without TSLAC IRT approval.
- Users must not install network hardware or software that provides network services without TSLAC IRT approval. Users are not permitted to alter network hardware in any way.
- Non-TSLAC computer systems that require network connectivity must conform to TSLAC IRT Standards.
- Users must not download, install or run security programs or utilities that reveal weaknesses in the security of a TSLAC system.

Password Policy

- The purpose of the TSLAC Password Policy is to establish the rules for the creation, distribution, safeguarding, termination, and reclamation of the TSLAC user authentication mechanisms.
- All passwords must be implemented according to the following TSLAC IRT rules:

❖ it must be routinely changed
❖ it must adhere to a minimum length as established by TSLAC IRT
❖ it must be a combination of alpha and numeric characters
❖ it must not be anything that can easily tied back to the account owner

such as: name, social security number, relative's names, birth date, etc.
- it must not be dictionary words or acronyms

- User accounts will be disabled when excessive invalid logon attempts are reached, and the account will be investigated before reinstated.
- User account passwords must not be divulged to anyone. TSLAC IRT and IRT contractors will not ask for user account passwords.
- If the security of a password is in doubt, the password must be changed immediately.
- Users cannot circumvent password entry with auto logon, application remembering, embedded scripts or hardcoded passwords in client software. 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 locking or logging off of the device.
- Passwords must be treated as confidential information

Creating a strong password

- Combine short, unrelated words with numbers or special characters. For example: eAt42peN
- Make the password difficult to guess but easy to remember
- Substitute numbers or special characters for letters. For example:
- livefish - is a bad password
- l!v3f1Sh - is far better, the capitalization and substitution of characters is not predictable

Portable Computing Policy

- The purpose of the TSLAC Portable Computing Policy is to establish the rules for the use of mobile computing devices and their connection to the network.
- Only TSLAC-approved portable computing devices may be used to access TSLAC Information Resources.
- Portable computing devices must be password protected.
- TSLAC sensitive or confidential data must not be stored on portable computing devices. In the event that there is no alternative to local storage, this data must be encrypted using approved encryption techniques.
- TSLAC sensitive or confidential 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.
- Non-TSLAC computer systems that require network connectivity must conform to TSLAC IS Standards and approved by the IRT Division.
- 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.

Security Training Policy

- The purpose of the TSLAC Security Training Policy is to establish the requirements to ensure that each user of TSLAC Information Resources receives adequate training on computer security issues.
- All new users must attend approved Security Awareness training prior to being granted access to any TSLAC information resources. Amended (04-24-2012) – Vendors are exempted from this requirement.
- All users must sign an acknowledgement stating they have read and understand TSLAC computer security policies and procedures. Vendors acknowledge that they have read and understand this summary.
- All users must attend annual computer security compliance training and pass the associated examination. Amended (04-24-2012) – Vendors are exempted from this requirement.

Software Licensing Policy

- The purpose of the TSLAC Software Licensing Policy is to establish the rules for licensed software on TSLAC Information Resources.
- Only appropriately licensed software is used on TSLAC resources. A sufficient number of licensed copies of software are provided. Management will make arrangements with appropriate vendors for additional copies if/when such are needed for business activities.
- Third party copyrighted information or software, that TSLAC does not have specific approval to store and/or use, must not be stored on TSLAC systems and will be removed by system administrators.

- Third party software in the possession of TSLAC can only be copied if such copying is consistent with relevant license agreements.
- Only authorized personnel can install software.
- Licensed material remains the intellectual property of the copyright holder at all times and is subject to the licensing terms.

Virus Detection Policy

- All workstations whether standalone or connected to the TSLAC network, must use the IRT approved virus protection software.
- The virus protection software must not be disabled or bypassed.
- The settings for the virus protection software must not be altered in a manner that will reduce the effectiveness of the software.
- The automatic update frequency of the virus protection software must not be altered to reduce the frequency of updates.
- Every virus not automatically cleaned by the virus protection software constitutes a security incident and must be reported to the Help Desk.

VPN Policy

- VPN privileges must be requested by the employee's director. Vendor VPN access must also be requested by the division director as the owner of the particular data/system for which the access is requested. VPN access is for agency business only. It is the responsibility of employees/vendor with VPN privileges to ensure that unauthorized users are not allowed access to the TSLAC network.
- The VPN user is responsible for selecting an Internet Service Provider (ISP), installing required software, and paying associated fees for Internet access except as otherwise provided by TSLAC policy.
- VPN users will follow the same Acceptable Use and Data Management Policies as when they use an internal connection to the network.
- Only TSLAC approved computing devices may be used to access TSLAC Information Resources. By using personal equipment, users must understand that their systems are a de facto extension of the TSLAC network during that connection and, as such, are subject to the same rules and regulations that apply to TSLAC-owned equipment.
- Only TSLAC-approved VPN client software may be used on the remote computer to connect to the agency's VPN.
- When using a VPN connection to access the TSLAC network, unattended computing devices must be physically secure.

Data Management Policy

TSLAC must manage the use of its data assets. To ensure the security of the data that the agency collects, produces, processes, and uses, TSLAC must identify the data assets, classify these assets according to their sensitivity to loss or disclosure, and identify the data owners, custodians, and users. The Data Management Policy provides a framework for data classification and the responsibilities of the owners, custodians, and users in managing this data. Data owners, custodians, and users must be aware of the classification of the data that is being accessed and must take steps to safeguard that data in accordance with that classification.

Classification Standard

Data shall be classified as follows:

Confidential. Sensitive data that must be protected from unauthorized disclosure or public release based on state or federal law (e.g., the Texas Public Information Act) and other constitutional, statutory, judicial, and legal agreements.

Examples of Confidential data may include but are not limited to:

- Personally Identifiable Information, such as: a name in combination with Social Security Number (SSN) and/or financial account numbers
- Intellectual Property, such as: Copyrights, Patents and Trade Secrets
- Medical Records

Agency-Sensitive. Sensitive data that may be subject to disclosure or release under the Texas Public Information Act, but requires additional levels of protection.

Examples of Agency-Sensitive data may include but are not limited to:

- TSLAC operational information and/or internal communications
- TSLAC personnel records
- TSLAC information security procedures

Public. Information intended or required for public release as described in the Texas Public Information Act.

Exception.

Information owned or under the control of the United States Government must comply with the federal classification authority and federal protection requirements.

Data Ownership Practice Standard

- The director of the division that collects the data is typically designated the Owner of the data. The data owner is responsible for the business results of the system or the business use of that data. The owner establishes the level of controls required to protect the data asset.
- The IRT division is typically designated as the Custodian of data assets. The custodian implements the controls specified by the owner; provides physical and procedural safeguards for the data assets; evaluates cost-effectiveness of controls; and implements monitoring procedures.
- A user is any person who has been authorized to read, enter, or update the data. The user uses the data for defined purposes only; complies with established controls; and prevents disclosure of confidential or sensitive data. A user must be aware of the classification of the data that is being accessed and must take steps to safeguard that data in accordance with that classification.
- The Assistant State Librarian is the Agency Information Security Officer (ISO). However, in order to allow the technical staff to act without delay on security matters, the IRT Network Operations Coordinator is the designated ISO for daily operations. The ISO recommends policies to executive management and establishes procedures in cooperation with owners and custodians to ensure the security of information resources assets against unauthorized or accidental modification, destruction, or disclosure.

(5) The agency head or designated representative reviews and approves ownership of information resources and associated responsibilities.

Disciplinary Actions

Violation of these policies may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; or dismissal for interns and volunteers. Additionally, individuals are subject to loss of TSLAC Information Resources access privileges, civil, and criminal prosecution.

Signature Date

Printed Name & Title

Organization Name

Appendix H
Vendor Security Policy Acknowledgement Form

Texas State Library and Archives Commission

I acknowledge that I have received, reviewed, and will comply with the *Texas State Library and Archives Commission's Vendor Information Resources Security Policy Summary*.

The Texas Administrative Code (TAC) Chapter 202 establishes the information Security Standards for Texas state agencies. This summary is based on the requirements of TAC 202.

I understand that it is my responsibility to use my best efforts to protect TSLAC data from disclosure to any unauthorized person.

The Information Resources Security Policies and, therefore, this policy summary, are subject to change through action by State Library management, the Texas State Library and Archives Commission, or the Texas Legislature.

Organization Name

Print Name Date

Signature

(Reviewed 01-29-2014 M.Alvarez)