Information Security Policy
End User Agreement

Regulatory Compliance

Office of Technology Services
Information Security and Compliance

State of Louisiana

Revision: 2.00
Date: January 7, 2025

Table of Contents

Overview

The State of Louisiana is entrusted with sensitive, proprietary and confidential information, including but not limited to; Protected Health Information (PHI), Federal Tax Information (FTI), Criminal Justice Information (CJI), and Personally Identifiable Information (PII). The state recognizes the importance of taking necessary actions to protect this information. One critical step in this process is ensuring that users of the State's information take responsibility for the protection and appropriate use of the State's information in accordance with the State's Information Security policies and procedures. Effective protection of such information requires the participation and support of every State employee, contractor and third-party affiliate. It is the responsibility of every User to acknowledge and follow the guidelines in this Policy.

Purpose

The purpose of this Policy is to provide guidance for the acceptable use of computer equipment and information within an Agency. Inappropriate use can expose the State to risks such as data loss, data corruption, unplanned service outages, unauthorized access to Agency data, and potential legal liabilities.

Scope

This policy applies to all Users, including State employees, independent contractors and all other workers at an Agency, including all personnel affiliated with third parties. This policy applies to all computing systems, electronic media and printed materials that are utilized, owned, managed, or leased by an Agency or the Office of Technology Services (OTS).

The Chief Information Security Officer (CISO) or a designated representative conducts an annual review of this document to ensure compliance with state and federal regulations, and security safeguards and standards. This document is updated annually, or whenever there is a significant change or security event.

Roles and Responsibilities

OTS is responsible for the development, dissemination, protection, and enforcement of information security standards outlined in this document and the Information Security Policy (ISP).

- Statewide Chief Information Security Officer (CISO): The CISO is responsible for the maintenance and implementation of the ISP, as well as all associated policies and procedures, including the Access Control. The CISO works with various operational sections, assurance functions, state agencies, and internal and external parties to implement, monitor, and evaluate the ISP and relevant associated policies and procedures.
- Information Security Team (IST): The IST is comprised of the CISO and specifically selected OTS resources with the primary responsibility of performing operational information security functions. Lead by the CISO, the IST works with applicable OTS, Agency, and Third-Party resources to develop, implement, communicate, and apply the ISP and associated policy and procedure, including Access Control, to State systems, data, and processes.

- Information Compliance Team (ICT): The role of ICT is to ensure State and Federal regulatory compliance requirements and controls are addressed and correctly implemented. ICT works with applicable OTS, Agency, and Third-Party resources to develop, implement, communicate, apply, and ensure appropriate risk mitigations and security controls are properly applied. ICT works with applicable OTS, Agency, and Third-Party resources to ensure Plans of Action and Milestones (POA&M), Corrective Action Plans (CAP), and other documentation are reviewed, prioritized, and mitigated in a timely manner.
- Information Security Officers (ISO): The CISO will assign specific members to serve as an ISO. An ISO will assist in leading information security initiatives related to specific regulatory environments. An ISO will also function as a dedicated resource for agencies to assist with planning, audits, incident response, notifications, and ensure regulatory requirements are implemented in a verifiable manner.
- System Administrators: Implement access control technologies, including the creation, modification, and removal of user access rights, in accordance with the Access Control Policy.

Policy

General Requirements

All Users are responsible for exercising good judgment regarding use of State resources in accordance with State's Information Security policies and procedures. The State's resources may not be used for any unlawful purpose. If you have a question regarding the proper use of technical resources, contact the Information Security Hotline at 844-692-8019.

All State systems, including handheld or mobile devices, computing devices, operating systems, applications, storage media, network accounts, Internet, Intranet, Extranet, and remote access are the property of State. These systems must be used for business purposes in serving the interests of State, and of Agency representatives in the course of normal operations.

Any personal device used in serving the interests of State, must be approved by applicable Agency leadership and the Information Security Team (IST).

Any data created or stored on Agency computing systems remains the property of the Agency. Any personal use of the Agency systems, including any documents or emails, are also the property of the Agency and the State makes no guarantee as to the confidentiality of personal use of Agency systems.

For security, compliance, and maintenance purposes, authorized personnel may monitor and audit Agency computing systems and networks per the State's policies and procedures.

All users must comply with Agency, State, and Federal policies, procedures and regulations regarding the access, use and safeguarding of data. Any questions about the appropriateness of data access or protection mechanisms should be directed to your supervisor or State contact.

User Accounts

The State's Users are responsible for the security of data, accounts, and systems under their control. It is crucial to keep passwords secure and do not share account or password information with anyone. For

example, do not write passwords down, do not email passwords and always use complex passwords (e.g., at least fourteen (14) characters long using a combination of lower case, upper case, numbers, and special characters).

Providing access to another individual, either deliberately or through failure to secure its access, is a violation of this Policy. If you believe that you have been granted access to systems or data outside the scope of your employment responsibilities or job function or if you have a question regarding the proper use of technical resources, please contact the Information Security Hotline toll free at (844) 692-8019.

Computing Systems

Users are responsible for ensuring the protection of assigned computing devices, including any electronic devices such as laptops, PDAs, mobile devices, and electronic media. Users are also responsible for ensuring the protection of any personal devices used in the interest of the State.

State Employees using either a State vehicle or their personal vehicles to transport the State's Computing Systems should exercise the utmost caution to safeguard the privacy of and access to such devices. At no time should such equipment be left on car seats, in plain view, in unlocked vehicles or stored in vehicles overnight.

Computing Systems that are stored overnight at non-State facilities must be protected with reasonable assurance of security to safeguard the data residing on the Systems.

Users of Agency Computing Systems must promptly report any theft or loss to the End User Computing (EUC) Support Services by calling locally at (225) 219-6900 or toll free at (844) 219-6900.

Security and Access Requirements

- All State Computer Systems or Agency approved personal devices used for State business purposes (e.g., PCs, laptops, workstations, smartphones, etc.) must be secured with a password-protected screensaver with the automatic activation feature set to activate within fifteen (15) minutes or less of inactivity.
- Users shall not create new passwords that are similar to passwords that have been previously used; create passwords that contain any reference to the State in any form (i.e., Pelican, Saints, etc.); create passwords that contain any personal data such as any portion of the user ID or name, a spouse's name, or a pet's name; or create passwords that appear in the dictionary.
- Users should secure their workstations by logging off or locking (*ctrl-alt-delete* or *Windows Key + L*) the device when unattended.
- Users must use due care when transmitting or storing sensitive information. Communications outside of an Agency Network should use mechanisms approved by the IST for protecting Confidential or Restricted data (e.g., encryption).

- Portable computers are especially vulnerable and will be protected by a current Antivirus solution and Personal Firewalls, installed or approved by OTS, and may not be disabled or modified by Users.
- Users must use extreme caution when accessing electronic media received from outside the State.
- Users shall take the necessary and appropriate precautions when opening attachments or emails and shall not open or click on attachments or emails when unsure of the legitimacy of the source or sender.
- Known incidents or infections from a virus, malware, or other malicious software should be immediately reported to IST.
- Streaming media should only be accessed for business purposes from trusted commercial sites. All other streaming media is prohibited.
- Meeting hosts should verify that all meeting attendees are authorized access to information shared during meetings (including online meetings). Remote meetings security features, such as pass codes or passwords, should be used to restrict access to the meeting to only authorized individuals. Remote meeting presenters should take care to close, or protect, Confidential or Restricted data while in "desktop sharing" mode.
- Users will take reasonable steps to protect all State property and information from theft, damage, or misuse. This includes maintaining and protecting User workspace, equipment, and information from unauthorized access whether working at Agency facilities or offsite.
- Users must use only authorized Instant Messenger clients; all other forms of instant messenger software are prohibited.

Newsrooms, Social Media Sites, and Social Networking Sites

Postings by Users regarding Agency business information or news to newsgroups, chatrooms, Internet Relay Chat (IRC), social networking or social media sites, artificial intelligence (AI), or code repositories (e.g. mIRC, Usenet, Facebook, X(Twitter), LinkedIn, Reddit, Pastebin, Stack Overflow, GitHub, Discord, ChatGPT, Copilot, Grok, Gemini, etc.) is strictly prohibited unless as legitimate job responsibilities or expressly approved in writing by the Agency Communication Director or Executive Leadership. If the User identifies himself or herself as employee or agent of the Agency on any Internet site, any postings to such sites must contain a clear disclaimer that the opinions expressed are solely those of the author and do not represent the views of the Agency or the State of Louisiana.

Virtual Private Network (VPN) Usage

It is the responsibility of users with VPN privileges to protect their VPN login and account information.

Connections to State resources via the VPN must originate from Agency authorized end user devices.

Users understand and acknowledge that by using VPN technology the connected computing resource is a de facto extension of the State's network, and as such is subject to the same rules and regulations that apply as if connected locally to the network.

Connections to non-State VPNs from within a State network must be specifically authorized by IST.

Physical Security

A State issued Identification badge must be worn on your person in a visible location at all times within a State facility. The identification badge must be properly secured and a lost badge must be immediately reported to the IST.

Do not facilitate the entry of non-badge personnel at any time. All visitors must check in at the reception area, clearly wear the Visitor badge at all times, and remain with their designated escort at all times. Guests are not allowed in the State facilities after hours except with the specific authorization of Agency leadership.

Individuals with Agency provided equipment must take appropriate measures to protect the equipment from theft, unauthorized use, or other activity that violates the State's ISP.

Individuals with access to Confidential or Restricted data should maintain a clean desk, pickup printed materials in a timely manner and appropriately secure paper-based documents when they are not in use.

Privileged User Accounts

Users with privileged user accounts (e.g., administrator or super-user accounts) must agree to the following:

- Individuals with Privileged User Accounts understand it is their responsibility to comply with all security measures necessary and assist in enforcing the ISP.
- Privileged User Accounts may only be used for valid business functions that require privileged access. Privileged account users must still abide by the least privilege principal and must not access or alter data for which they have no valid business reason to do so.
- Individuals will login to an Agency environment using standard user credentials and then log in to a specific privileged account, except when logging directly into a system interface console.
- Privileged user accounts may not be used to modify the individual's standard user account.
- Privileged user accounts must comply with requirements of the ISP prior to modifying any system or user account.
- Individuals with privileged user accounts understand and acknowledge that all privileged user account activity is closely monitored. Individuals with privileged user accounts may not use those accounts to modify, alter, or destroy monitoring log data, except as required by their position responsibility as it relates to log rotation.

Unacceptable Use

The following activities are, in general, prohibited. To the extent a State User needs to be exempted from one of the following restrictions for legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services), that State User will be provided express authorization from the IST. The activities below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

- Engaging in any activity that is illegal under local, federal, or international law.
- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the State of Louisiana.
- Unauthorized copying of copyrighted material including digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the State or the end user does not have an active license is strictly prohibited. The use of any recording device, including digital cameras, video cameras, and cell phone cameras, within the premises of any State properties to copy or record any Internal, Confidential, or Restricted data is prohibited.
- Connecting network devices such as wireless access points or personal laptops into the State's network environment without proper authorization from IST.
- Intentional introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, email bombs, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using an Agency computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any State issued user account.
- Effecting security breaches or disruptions of network communication. Security breaches include accessing data of which the individual is not an intended recipient or logging into a server or account that the individual is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes degrading the performance, depriving authorized access, disabling or degrading security configurations.

- Port scanning or security scanning is expressly prohibited unless prior approval is granted by the IST.
- Executing any form of network monitoring which will intercept data not intended for the user's host, unless this activity is a part of the user's normal job or duty.
- Circumventing user authentication or security of any host, network or account.
- Interfering with or denying service to any User (e.g., denial of service attack).
- Intentionally restrict, disrupt, impair, or inhibit any network node, service, transmission, or accessibility.
- Utilizing unauthorized peer-to-peer networking or peer-to-peer file sharing.
- Utilizing unauthorized software, hardware, proxy avoidance websites or services, or any other means to access to any internet resource or website that has been intentionally blocked or filtered by the State, Agency, or IST.

Email and Communications Activities

- Sending non-business-related unsolicited email messages, text messages, instant messages, or voice mail, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Engaging in any form of harassment or discrimination through email or other electronic means.
- Use of personal email account from the State networks.
- Forging, misrepresenting, obscuring, suppressing, or replacing a user identity on any electronic communication to mislead the recipient about the sender.
- Soliciting email for any other email address (e.g., phishing), other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding chain letters, Ponzi or other pyramid schemes to a State User, unless specifically requested by such State User.
- Posting non-business-related messages to a large numbers of Usenet newsgroups (newsgroup spam).
- E-mail may not be stored on personal devices (e.g., home computers, personal laptops, PDA's, Smartphones, etc.) except as authorized by IST.
- Text messages should not to be used for business discussions. Confidential and Restricted data shall not be communicated over text messaging.

References

OTS Information Security Policy (ISP)

Owner

Division of Administration, Office of Technology Services, Information Security

Contact Information:
Information Security Hotline Toll Free: (844) 692-8019
OTS Information Security Team - InfoSecTeam@la.gov
OTS Information Security Compliance Team – InfoComp@la.gov
OTS User Support - OTSSupport@la.gov

Approved by: Donny J. Brown, IT Statewide Director Date: 01/07/2025
Effective Date: 01/07/2025

Revision History

Version	Date	Description	Author
1.00	01/01/2015	Creation.	Information Security Compliance
1.02	01/13/2022	Updated EUA.	Paula Sobolewski
2.00	12/17/2024	Reformatted using new OTS Brand Guide and matched verbiage to SuccessFactors Training.	Marnie Cook
2.00	01/03/2025	Reviewed and updated.	Carla Simoneaud
2.00	01/07/2025	Review, update and approved.	Donny Brown

IMPORTANT NOTE: The Chief Information Security Officer oversees actions to create, monitor, and enforce Statewide Information Technology policies and procedures, and identify and address vulnerabilities and risks, and manage security incidents. Consequently, the policy and procedures are reviewed and updated by Information Security Compliance Team to ensure federal regulations and safeguards are met. Any user found to have violated Office of Technology Services Information Security policies and procedures may be subject to disciplinary action, up to and including dismissal, or criminal or civil legal actions.

End User Agreement Attestation

- By signing this Agreement, Users acknowledge that they are aware of and understand the State's policies regarding the privacy and security of individually identifiable health, financial, criminal and other personal information of individuals and employees, including the policies and procedures relating to the use, collection, disclosure, storage, and destruction of Confidential and Restricted data.
- In consideration of Users' employment or association with the State and as an integral part of the terms and conditions of such employment or association, Users covenant, warrant, and agree that they shall not at any time, during their employment, contract, association, or appointment with the State or after the cessation of such employment, contract, association, or appointment, access or use Confidential or Restricted data except as may be required in the course and scope of their duties and responsibilities and in accordance with applicable law and corporate and departmental policies governing the proper use and release of Confidential or Restricted data.
- Users must understand and acknowledge their obligations outlined hereinabove will continue even after the termination of employment, contract, association, or appointment with the State.
- Users must also understand that the unauthorized use or disclosure of Restricted data shall result in disciplinary action up to and including termination of employment, contract, association, or appointment, the institution of legal action pursuant to applicable state or federal laws, and reports to professional regulatory bodies.
- Users further acknowledge that by virtue of their employment, contract, association, or appointment with the State, they may be afforded access to Confidential and/or Restricted Information concerning the operations and practices of a State Agency, which shall specifically include, but shall not be limited to inventions and improvements, ideas, plans, processes, financial information, techniques, technology, trade secrets, manuals, or other information developed, in the possession of, or acquired by or on behalf of the State, which relates to or affects any aspect of Sate's operations and affairs. Users agree that they will not use, disclose, or distribute Confidential Information or information derived therefrom except for the exclusive benefit and permission of the State Agency.
- Users understand, acknowledge, and agree that nothing contained herein shall be deemed or regarded as an employment contract or any other guarantee of employment, and shall not otherwise alter or affect User status as an at-will employee (or where applicable, independent contractor) of the State.

Enforcement

Any User found to have violated this End User Agreement Policy may be subject to disciplinary action, up to and including dismissal, or criminal or civil legal actions.

The State Employee is required to provide the information below and sign the document.
If the individual is a Contractor, both the Contractor and the sponsoring State Employee must provide the information below and both must sign the document

	State Employee	Contractor
Name:		
Title:		
Agency:		
Phone:		
Email:		
Signature:		
Date:		