GOVERNANCE

This document is governed by the IT Governance policy which provides the following guidance:

a. Roles and Responsibilities
b. Policy Control Application
c. Policy Compliance Requirements
d. Policy Exceptions and Exemptions
e. Policy Reviews and Updates

SCOPE

This policy provides the security awareness and training requirements establishing best practices to secure State of Alabama information assets based on State law, rules, regulations, and requirements contained in the State's IT Governance Policy, and covers all State information and systems accessed, managed, or operated by a contractor, agency, or other organization on behalf of the State. This applies to all employees, contractors, and any users of information and systems supporting the operation and assets of the State.

AT-1 POLICY AND PROCEDURES

This document addresses the requirements set forth by the State to implement the family of Awareness and Training security controls at the organization, process, and/or system level for all information assets.

The State has adopted the Assessment, Authorization and Monitoring principles established from the NIST SP 800-53 "Awareness and Training," control guidelines, as the official policy for this security domain. The "AT" designator identified in each control represents the NIST-specified identifier for the Awareness and Training control family. A designator followed by a number in parenthesis indicates a control enhancement that provides statements of security and privacy capability that augment a base control. Only those control enhancements associated with the moderate level controls are listed. Should an executive-branch agency be required to address other control enhancements for a control item, the organization will be responsible for writing an additional policy to meet that requirement.

The State requires all users, including contractors, of its managed systems and information to receive security awareness training at hiring, and annually thereafter, to ensure each user's familiarity with State information security policies.

As such the State shall:

a. Provide employees and contractors with mandatory information security training at job hiring and provide regularly recurring information security awareness communications to all employees and contractors by various means, such as but not limited to digital/electronic updates, briefings, and newsletters; and
b. Ensure all users of implemented systems are trained on appropriate and secure use of those systems and how they will impact each user's current roles and responsibilities.

This policy and standards shall be reviewed and updated at least every three (3) years, or as State-determined events necessitate an earlier review. Agency senior management will ensure information security communications are prioritized by staff and will support information security awareness programs.

AT-2 SECURITY TRAINING AND AWARENESS

Agencies shall provide organizational-specific cybersecurity and privacy training beyond State-required training and provide the relevant cybersecurity and privacy best practices information to all system users as needed. An auditable log of user training completions indicating as least pass/fail feedback shall be implemented and maintained.

Training methods and requirements include, but are not limited to:

a. A summary of cybersecurity and privacy policies with a verifiable tracking and delivery method will be sent to all system users for their signature indicating understanding and acceptance of the policies.
b. Role-based or duty specific formal cybersecurity and privacy training will be provided annually or more frequently as required.
c. Prevention of access to sensitive or confidential data (see Data Classifications in IT Governance Policy) until initial role based or duty specific training is complete. User training shall be provided when required by system changes or agency-defined events require such training.
d. Information security and privacy needs shall be reassessed when staff members change jobs or roles, and subsequent training in procedures or proper use of information-processing facilities will be prioritized.
e. Agencies shall use interactive training modules, cybersecurity newsletters, or other media awareness techniques necessary to increase the security and privacy awareness of system users.

AT-2 (2) SECURITY TRAINING AND AWARENESS - INSIDER THREAT

An insider threat is an entity having authorized access with potential to harm an information system or enterprise through destruction, disclosure, data modification, and/or denial of service.

Insider threat training on how to recognize, prevent, detect, and report potential inside threats via appropriate State channels shall be provided as required by policies and procedures.

Examples of insider threat are behaviors such as attempts to gain elevated information access not required for job performance, unexplained access to financial resources, bullying or sexual harassment, workplace violence, and other serious violations of State policies, procedures, directives, rules, or practices.

AT-2 (3) SECURITY TRAINING AND AWARENESS – SOCIAL ENGINEERING AND MINING

Social engineering attempts to trick an individual into revealing information or taking an action causing a breach, compromise, or otherwise adversely impacting a system. Samples are phishing, baiting, impersonation, social media exploitation, and tailgating. Social mining attempts to acquire agency information to support a future attack.

Training on recognizing and reporting potential and actual instances of social engineering and social mining shall be provided. Some examples of this training include:

a. Simulated phishing as a test.
b. Distributing phishing email samples.
c. Distributing real-world examples of successful mining/phishing consequences.

AT-3 ROLE-BASED TRAINING

Security and privacy-related training shall reflect individual responsibility for using, configuring, and/or maintaining information systems, as well as reflect the privacy requirements of the State. Training in critical areas of physical security, cybersecurity, and privacy, including vendor-specific safeguards, will be provided to users and technical staff.

Role-based training will include the following:

a. Role-based security and privacy-related training shall be provided before authorizing a person's access to a system and before they are allowed to perform their assigned duties when required by system changes.
b. Role-based training content will be updated annually and/or after agency-defined events requiring update.
c. Lessons learned from security or privacy incidents shall be used in role-based training.
d. Cybersecurity threats and safeguards training with technical details reflecting the staff's individual responsibility for configuring and maintaining information security is required.
e. Information security and privacy professionals requiring additional expertise in security and privacy for their duty roles will receive additional training as needed through formal external courses and certification programs.

AT- 4 TRAINING RECORDS

The State shall document and monitor individual security and privacy training activities, including basic security awareness training and specific role-based information system security and privacy training, and retain these records for five (5) years from date of test.

AT-6 TRAINING FEEDBACK

State management shall solicit feedback from agency training managers or agency POC for Awareness and Training responsibilities to provide more targeted training based on developing data regarding the relevance and effectiveness of the security and privacy awareness training provided by the State, particularly training that may be role-specific due to quickly evolving technology and subsequent emerging threats.

POLICY OWNER

Secretary of Office of Information Technology (OIT)

MATERIAL SUPERSEDED

This current policy supersedes all previous versions. All State agencies and contractors/vendors of the State are expected to comply with the current implemented version.

REVISION HISTORY

Revision Date	Summary of Change
12/31/2024	Policy Update

REMAINDER OF PAGE LEFT INTENTIONALLY BLANK

APPROVED BY

Signature	Daniel Urquhart
Approved by	Daniel Urquhart
Title	Secretary of Office of Information Technology (OIT)
Date Approved	01/15/2025

REMAINDER OF PAGE LEFT INTENTIONALLY BLANK