STATE OF ALABAMA

Information Technology Policy

POLICY 610-02: CYBER SECURITY AWARENESS AND TRAINING

Security across multiple hardware and software platforms requires security-aware users as well as a well-trained technical staff. Awareness and training are key elements of a successful cyber security program, but awareness differs from training. The goal of awareness is to reach a broad audience to focus attention on security. Awareness level training increases recognition of the need to protect data and creates sensitivity to data and information system threats and vulnerabilities. Training is more formal. The goal of training is to build the knowledge and skills needed to facilitate individual job performance. Security training is essential for the people who operate and support existing systems, design and deploy new systems, or require advanced specialty skills (such as digital forensics).

OBJECTIVE:

Ensure all information system users receive timely cyber security awareness and training, appropriate to their roles and responsibilities, to increase awareness of information security risks, increase technical competence, and ensure compliance with information security policies and standards.

SCOPE:

This policy applies to all Executive Branch agencies, boards, and commissions except those exempt under The Code of Alabama 1975 (Title 41 Chapter 4 Article 11).

RESPONSIBILITIES:

Agency Management, Information Technology Organization:

Each agency shall develop, document, and implement an agency-wide cyber security program to provide information security awareness and training pertaining to the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. Cyber security programs shall include:

(1) security awareness to inform all personnel, including contractors and other users of information systems that support the operations and assets of the agency, of:

(a) information security risks associated with their activities; and

(b) their responsibilities in complying with State and agency policies and procedures designed to reduce these risks; and

(2) on-going security training for information systems support personnel, system administrators, and security managers appropriate to their roles and responsibilities.

Security awareness and training procedures shall be developed for the security program in general and (when required) for a particular information system.

Ensure all system users are exposed to basic information system security awareness materials before authorizing access to the system and at least annually thereafter.

Identify personnel with significant information system support roles and responsibilities, document those roles and responsibilities, and provide appropriate information system security training before authorizing access to the system and at least annually thereafter.

Determine the appropriate content of security awareness and training based on the specific requirements of the organization and the information systems to which personnel have authorized access.

Document and monitor individual information system security awareness and training activities.

ADDITIONAL GUIDANCE:

Security awareness topics may include (but are not limited to):

- Policies and Standards and where to find them
- Password usage and management – creation, frequency of changes, and protection
- E-mail usage – handling attachments, prohibited use, mass mailings
- Web usage – access, prohibited use, monitoring of user activity
- Malware Protection – viruses, worms, Trojan horses, and other malicious code
- Vulnerability Management – timely application of system patches
- Spam
- Social engineering
- Incident response – reporting and handling
- Physical Security – facility access, visitor control, environmental risks, etc.
- Desktop security – allowed access to systems, use of screensavers, restricting view of information on screen (preventing "shoulder surfing"), device locking
- Laptop security – both physical and information security issues
- Handheld device security – both physical and wireless security issues
- Individual accountability – identification and authentication; access to systems and data
- Access control issues – least privilege, separation of duties, etc.
- Using personally owned systems at work or connecting remotely
- Software licensing and use
- Data backup and storage
- Information Protection – confidentiality concerns and controls
- Encryption – transmission and storage of sensitive/confidential information
- Information System Disposal – property transfer, media sanitization

The following topics at a minimum should be addressed as baseline security training for all technical support personnel (system administrators, security administrators, network administrators, etc.):

- Protecting systems from malware
- Data backup and storage
- Timely application of system patches
- Configuration/change management
- Access control measures
- Network infrastructure protection measures

National Institute of Standards and Technology (NIST) Special Publication 800-16: Information Technology Security Training Requirements: A Role- and Performance-Based Model, and NIST Special Publication 800-50: Building an Information Technology Security Awareness and Training Program provide guidance on developing security awareness and training programs.

By Authority of Director, Information Services Division, Department of Finance

DOCUMENT HISTORY:

Version	Release Date	Comments
610-01	12/5/2005	Original
610-01_A	1/12/2007	Completely revised.
610-02	09/01/2011	Incorporated contents of Standard 610-01S1 (hereby rescinded).