



KAY IVEY  
Governor

# STATE OF ALABAMA

## OFFICE OF INFORMATION TECHNOLOGY



JIM PURCELL  
Acting Secretary

### POLICY 640: Security Awareness and Training

VERSION NUMBER	Policy 640-01
VERSION DATE	March 15, 2018
POLICY TITLE	Security Awareness and Training
OBJECTIVE	To educate all State of Alabama employees, who have access to State information technology (IT) resources, about their information security and privacy roles and responsibilities in support of published security policies, standards, and procedures, and to ensure the protection of the confidentiality and integrity of sensitive data collected or maintained by the State.
AUTHORITY	<p>The authority of the Office of Information Technology (OIT) to create and enforce policies relating to the management and operation of IT by state agencies, and exceptions to such authority, are derived from:</p> <p><i>Articles 8 and 11 of Chapter 4 of Title 41, and Chapter 28 of Title 41, Code of Alabama 1975 (Acts 2013-68 and 2017-282).</i></p> <p>Policies of the OIT are approved and signed by the Governor.</p>
APPLICABILITY	The requirements and responsibilities defined in OIT policies apply to all departments, agencies, offices, boards, commissions, bureaus, and authorities (referred to generally as “agency” or “agencies”) and authorized individuals in the employment of the State responsible for the management, operation, or use of State of Alabama IT.

## STATEMENT OF POLICY

It is the policy of the OIT that State personnel, employees, and contractors who have access to State IT must complete IT Security Awareness Training:

- a) Before authorizing access to the IT or performing assigned duties; and
- b) no less than annually thereafter; and
- c) when required by information system or user role changes.

If training is computer-based, and network access is required to complete training, the new employee may be given limited network access (i.e., access to the public Internet or training environment only) for the sole purpose of completing said training.

At a minimum, IT Security Awareness Training shall cover the following topics:

- Cloud Use and Access
- Data Destruction
- Data Retention
- Data Security
- Email & Messaging
- Encryption
- Ethics
- Insider Threat
- Internet Browsing
- Mobile Device Security
- Passwords
- Persistent Threats
- Personally Identifiable Information (PII)
- Physical Security
- Privacy
- Protecting Your Personal Computer
- Social Engineering
- Social Networks
- Social Security Numbers
- Wi-Fi Security
- Working Remotely

Agencies may supplement user awareness training by adding topics that are pertinent to their organization.

OIT  
RESPONSIBILITIES

Identify security awareness programs, services, or applications that meet all requirements stated above.

Negotiate enterprise agreements with selected security awareness program vendors and offer program participation to state agencies at a fair and reasonable price.

AGENCY  
RESPONSIBILITIES

Establish, implement, and maintain an IT security awareness program, compliant with this policy for all employees of the agency; or, adopt and utilize the awareness program of the OIT. Agencies may supplement the OIT program with agency-required information.

Provide role-based security training to personnel with information system support roles and responsibilities (may include system administrators, software developers, configuration managers, and auditors/assessors, etc.):

- a) Before authorizing access to the IT or performing assigned duties; and
- b) no less than annually thereafter; and
- c) when required by information system or user role changes.

Document and monitor individual information system security training activities including basic security awareness training, specific information system security training, and specialized role-based training.

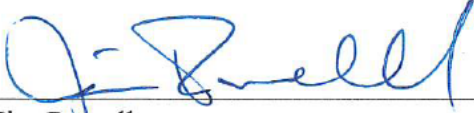
Retain individual training records for a period of no less than five years.

Agencies may determine where training record documentation is maintained.

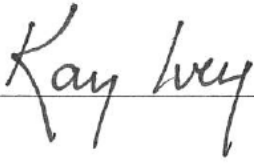
Agencies shall provide to OIT, upon request, reports indicating agency compliance with this policy.

USER RESPONSIBILITIES	Complete assigned training. Individuals may be denied access to State IT until they have complied with this policy.
SUPPORTING DOCUMENTS	<p>The following special publications (SP) of the National Institute of Standards and Technology (NIST) support this policy and may aid in its implementation:</p> <ul style="list-style-type: none"><li>• NIST SP 800-16: IT Security Training Requirements</li><li>• NIST SP 800-50: Building an IT Security Awareness and Training Program</li></ul>
EFFECTIVE DATE	This policy shall be effective upon its approval by the Secretary of Information Technology and the Governor of Alabama as evidenced by the signatures of the Secretary and Governor being affixed hereto.
SUPERSEDES	This policy supersedes OIT Policy 628-01 and ISD Policy 610 which are hereby rescinded.

The undersigned, as Acting Secretary of Information Technology of the State of Alabama, exercising the power vested in that Office by the laws of this State, declares this policy to be adopted as of the date on which the Governor has approved and signed it.

  
\_\_\_\_\_  
Jim Purcell  
*Acting Secretary of Information Technology*

ORDERED

  
\_\_\_\_\_  
Kay Ivey  
*Governor*

This 16<sup>th</sup> day of March, 2018.

DOCUMENT CHANGE HISTORY

Version	Version Date	Comments
640-01	03/15/2018	Initial version; supersedes OIT Policy 628 and ISD Policy 610