# State of New Mexico Statewide
# Architectural Configuration Requirement
# Title: Security Training and Awareness Standard
# S-POL-003.001
# Effective Date: August 18, 2005

## 1. Authority

The Department of Information Technology (DoIT) shall develop, implement and maintain a coordinated statewide plan for information technology (IT) including the adoption of statewide technical, coordination, and security standards per the Department of Information Technology Act, NMSA 9-27-1 et. seq. (1978).

## 2. Purpose

The purpose of this standard is to define criteria for a security training and awareness program at State agencies designed to educate State employees of the requirements to protect State information and IT resources and provide the knowledge and skills necessary to fulfill IT security responsibilities for the State.

## 3. Scope

This applies to all agencies. Agency is defined as a department, commission, board, institution or other agency of the state organization receiving, expending or disbursing state funds or incurring obligations of the state including the board of regents and the state board of directors for community colleges but excluding the universities under the jurisdiction of the board of regents and the community colleges under their respective jurisdictions and the legislative or judicial branches.

The Agency Chief Executive Officer, working in conjunction with the Agency Chief Information Officer, shall be responsible for ensuring the effective implementation of Statewide Information Technology Policies, Standards, and Procedures within each agency.

## 4. Standard

The following standards provide criteria for agency security awareness and training programs to clearly outline State employee responsibilities.

4.1. CONTENT: Security awareness training content shall be created and regularly reviewed, and updated, on a frequency determined and documented by the agency, to ensure that it addresses the agency's organizational mission, culture, business, technology, systems, and data/information.

4.1.1. Training material shall include, at a minimum, content that:

- Enables the individual to understand the meaning of IT security, why it is needed, and his/her personal responsibility for security along with the importance of complying with all Statewide and budget-unit-specific security policies and standards;
- Includes or references State of New Mexico Enterprise IT Security S-GUIDE-002, statewide security standards, and statewide policies for email and Internet use that establish basic, general rules of employee general rules of behavior into their own culture based on business services and requirements, to reduce the possibility for confusion or misunderstanding. Where agency IT security requirements are more stringent than Statewide IT security policies and standards, those elements should be clearly explained;
- Enables the individual to identify and evaluate threats, vulnerabilities, and risks specific to agency data/information and IT resources;
- Enables the individual to better understand social engineering persuasion techniques that may be used to deceive an individual into revealing confidential, private, or privileged information in order to compromise the confidentiality, integrity, and availability of agency data/information and IT resources;
- Includes technical alternatives, methods, and standards which represent best practices appropriate to agency data/information and IT resources, and which can be utilized to effectively implement safeguards, as appropriate; and
- Covers, but is not limited to:
    - The responsibility of individuals to report IT-security-related issues;
    - The fact that an individual's activities can be audited;
    - The legal requirements for data (citing legislation as appropriate);
    - Privacy expectations of State employees and third-party organizations;
    - The ownership of data;
    - Non-business use issues;
    - The agency's password requirements for usage and management;
    - Virus and malicious code protection;
    - Incident response procedures;
    - The enterprise acceptable use policy for email and Internet Use;
    - Encryption technologies and the transmission of sensitive/confidential information over the Internet;
    - The enterprise intellectual property and fair use requirements;
    - Supported/allowed software on agency systems;
    - The sensitivity of agency systems to threats, risks, and vulnerabilities;
    - Social engineering techniques commonly used to deceive users into giving away access or revealing confidential or privileged information;

- Physical security; and
- Applicability of security requirements to all IT resources, including portable IT devices, such as laptops, etc.

4.1.2. Security awareness training materials (manuals, documents, etc.) as well as IT security policies, standards, and procedures should be made readily available, either electronically or via hard copy, to all State employees.

4.1.3. Agencies should incorporate formal evaluation and feedback mechanisms to gauge the appropriateness and effectiveness of its security awareness and training programs, techniques, and materials.

4.2. ROLES AND RESPONSIBILITIES: Agencies should clearly define and document key personnel IT security roles and responsibilities. Contact information, as appropriate, should be included in security awareness and training manuals, documents, handouts, etc.

4.3. LEVEL OF AWARENESS AND TRAINING: The level of security awareness and training should be commensurate with the level of access and expertise required in relation to the system components and information resources for which the State employee is responsible.

- Security awareness and training should be incorporated into an agency's new hire training for every State employee.
- All State employees should receive security training prior to being provided any access to IT systems and resources. Prior to accessing State or agency specific software applications, employees should receive any specialized security training as appropriate focused for their role and responsibility relative to the software application system.
- The receipt of security awareness training should be documented in the employee's personnel file with the employee's acknowledgement of having received and understood the training.
- Security awareness shall be promoted on an on-going basis. State employees should have their security awareness training updated annually or upon occurrence of a specific event, such as a change in job responsibilities, employment status, etc.

4.4. LEVERAGE OF KNOWLEDGE: Agencies are encouraged to share their security awareness training programs and materials with other agencies.

# 5. Definitions

Refer to the N-DEF001.001 Glossary of Terms located on the DoIT website: http://www.doit.state.nm.us/standards.html

# 6. References

- State of New Mexico Enterprise Architecture, NMAC 1.12.11
- Internet, Intranet, Email, and Digital Network Usage, NMAC, 1.12.10
- State of New Mexico Enterprise IT Security, S-GUIDE-002
- Statewide Standard S-STD-001, Authentication and Directory Services
- Statewide Standard S-STD-002, Configuration Management
- Statewide Standard S-STD-003, IT Risk Management
- Statewide Standard S-STD-004, Account Management
- Statewide Standard S-STD-005, Network Security
- Statewide Standard S-STD-006, Virus and Malicious Code
- Statewide Standard S-STD-007, Session Controls
- Statewide Standard S-STD-008, Wireless Access Point Hardware
- Statewide Standard S-STD-009, IT Physical Security
- Statewide Standard S-STD-010, Backups
- Statewide Standard S-STD-011, Personnel Security
- Statewide Standard S-STD-012, Incident Response and Reporting

# 7. Attachments

None

# 8. Version Control

S-POL-003.002

# 9. Revision History

Original 08/18/05  
Format Updated 09/18/13