State of New Mexico Statewide Architectural Configuration Requirements
Title: Personnel Security Standard
S-STD011.001
Effective Date: June 2, 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

This standard defines requirements for protection of State IT assets from intentional misuse or destruction by State employees or contractors, who represent a potential source of unauthorized access and misuse of sensitive and confidential information.

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 standard provides requirements that protect information technology assets belonging to the State of New Mexico from misuse or destruction by State employees and contractors.

4.1. WRITTEN POLICIES AND PROCEDURES: Agencies shall establish and document personnel security policies as well as related procedures that show clear accountability for security administration. Policies and procedures shall be applied to every existing State employee and contractor, as well as to new State employees and contractors, in order to prevent potential unauthorized access to and misuse of sensitive and confidential information. Policies and procedures shall be made available to all State employees and contractors and should be signed to indicate acceptance and understanding.

The specific procedure which directs the steps and the timing required to grant or withdraw physical and system access privileges to State employees and contractors working for or on behalf of the agency shall be documented for the following events:

- New hire and/or new contractor staff/organization;
- Change of job duties within the agency;
- Transfer to another agency;
- Resignation;
- Termination, contract expiration; and
- Alleged inappropriate behavior (as defined by the agency).

4.2. DOCUMENTED ACCESS TO INFORMATION AND RESOURCES:

4.2.1 System, application, and information access shall only be granted in accordance with a formal, written, and auditable procedure (including a formal, written request for access to specific systems or data). Granting of access should be accompanied by appropriate security training; in accordance with Statewide Standard, Security Training and Awareness S- POL-003.

4.2.2 Statewide Standard, Account Management S-STD-004, provides requirements for establishing and changing user accounts, classifications, and responsibilities.

4.2.3 Users should be provided access to the minimum set of resources required for their role, to minimize the impact of any security violations and improve accountability. The principle of least privilege requires identifying what the user's job is, determining the minimum set of privileges required to perform that job, and restricting the user to those privileges and nothing more. Denying access to resources that are not necessary for the performance a user's duties prevents those denied privileges from being used to circumvent security policy and standards.

4.2.4 Permissions, or rights, shall be granted in accordance with group or role membership(s) based on job functions and assignments.

4.2.5 Access privileges shall be removed whenever an authorized user changes jobs or terminates employment.

4.2.6 Intellectual Property – access to intellectual property shall be granted only after fulfillment of requirements specified in [Statewide Intellectual Property and Fair Use].

4.2.7 E-mail – e-mail access shall only be established in accordance with requirements provided in Internet, Intranet, Email And Digital Network Usage, NMAC 1.12.10.

4.2.8 Internet Access – Internet access shall only be established in accordance with requirements provided In Internet, Intranet, Email And Digital Network Usage, NMAC 1.12.10.

4.2.9 SEPARATION OF DUTIES: Where reasonably and economically feasible for an agency, the State employee or contractor in charge of security for a "like" group of IT devices or services should not be

responsible for the security of other groups of IT devices or services. (For example, the individual establishing user accounts should not be the same individual that grants access to software applications and associated databases.)

4.3. EMPLOYMENT CONSIDERATIONS: Job-related requirements for potential IT personnel or contractors working in primary facilities housing critical information systems or handling confidential information shall be a hiring consideration.

4.3.1. Terms and conditions of employment and job descriptions should specify information security responsibilities.

4.3.2. IT personnel who will receive administrative access to network or database resources should be required to have a background check completed.

4.3.3. Agencies that perform fingerprint imaging shall adhere to current New Mexico Department of Public Safety (DPS) standards for fingerprint imaging/identification.

4.3.4. Non-Disclosure Agreements and applicable confidentiality and security agreements shall be signed by all State employees or contractors who require access to confidential information, prior to their being granting access to that information.

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

None

7. Attachments

None

8. Version Control

S-STD-011.001

9. Revision History

Original 06/02/05
Format Updated 09/19/13