State of New Mexico Statewide Architectural Configuration Requirements Title: Account Management Standard <u>S-STD004.001</u> Effective Date: April 7, 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 coordinate agency and State implementations for controlling and managing access to IT systems, applications, information, and resources.

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 Department Secretary, working in conjunction with the Department Chief Information Officer (CIO), shall be responsible for ensuring the effective implementation of Statewide Information Technology Policies, Standards, and Procedures (PSP) within each agency.

4. Standard

The following standards provide accountability and accounting requirements for creating and changing user accounts, authorizations, and responsibilities. In accordance with *Statewide Standard Personnel Security S-STD-011*, standards contained in this document shall apply to State employees and contractors.

4.1 Policies and Procedures

Agencies shall create and document policies and procedures for establishing on-line accounts, levels of approval, access to confidential information, remote access, monitoring inactive accounts, forgotten passwords, and closing accounts based on voluntary leave or termination.

4.2 Responsibility for Actions

Agencies shall establish, document, and communicate a policy requirement that accountability for actions taken on an IT resource (e.g., computer system, agency or State application system, etc.) belongs to the owner of the specific userID under which those actions take place.

4.3 Written Access Authorization

In accordance with Personnel Security Standard S-STD-011, system, application, and information access shall be granted via a formal and auditable procedure; have a retrievable, associated written record of the request and subsequent authorization; and should be accompanied by appropriate security training in accordance with Security Training and Awareness S-POL-003.

- A non-disclosure agreement shall be signed by any State employee or contractor who requires access to sensitive information, prior to being granted access to such information. Classification and categorization of data defines confidential information requirements and provides the opportunity for agencies to create and document additional classifications of data/information.
- Permissions, or rights, shall only be granted in accordance with the requestor's group or role membership(s).
- User authorization should be based on least privilege required to perform assigned tasks.
- Access privileges shall be removed whenever an authorized user changes jobs or terminates employment.

4.4 Documented Procedures

In accordance with Personnel Security, agencies shall document and maintain a procedure directing the steps and the timing for granting or withdrawing system and information access privileges.

- Events requiring action include: new hire, transfer to another agency, change of duties within the agency, resignation, termination, and report of alleged inappropriate behavior (as defined by the agency) by an employee.
- Events apply to agency employees and contractors.
- Thresholds for acceptable periods of inactivity for user accounts shall be documented and monitored. Inactive accounts meeting the determined thresholds shall be initially disabled and subsequently removed.
- Procedures to address requirements for issuing new passwords to replace forgotten passwords shall be documented and maintained.

4.5 Special Access Privileges

Agencies shall, in their procedures, document and maintain special access privileges, including high-level privileges (such as root access on distributed systems), system utilities, and privileges that provide access to sensitive network devices, operating system, or software application capabilities. Procedures shall include:

- Specifying and documenting the purpose of special access privileges.
- Restricting the use of special access privileges and requiring approval for use.
- Requiring identification codes or tokens that are different from those used in normal circumstances.
- Specifying and documenting a procedure to remove special access privileges.

4.6 Remote Access Users

In addition to requirements specified in paragraphs 4.1 through 4.5, the agency shall establish and document procedures to identify all holders of remote access privileges to agency IT resources, including third-party entities, such as suppliers, trading partners, etc. Lists of remote users shall be kept current.

4.7 Automated Administration

Tasks associated with account administration should be automated to reduce time and errors.

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-004.001

9. Revision History

Original 04/07/05
Format Updated 09/18/13