State of New Mexico Statewide Architectural Configuration Requirements Title: Session Controls Standard S-STD007.002 Effective Date: May 5, 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 efforts to prevent unauthorized access to critical systems via workstations left unattended. Unattended workstations logged into networks, systems, and applications may allow unauthorized access to critical 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 (PSPs) within each agency.

4. Standard

The following session controls provide minimum requirements for preventing unauthorized access to information, systems, applications, and networks via unattended workstations at agencies, regardless of location, throughout the State. Requirements shall be documented and maintained as part of, and in accordance with, Statewide Standard, Account Management S-STD-004.

4.1. SESSION/SYSTEM TIMEOUT**:** Agencies shall develop, implement, and communicate procedures for:

- Automatic session timeouts to be in place on multi-user information

systems and remote communication systems, with the maximum period of inactivity set commensurate with the sensitivity of information housed on the individual system.

- All system users should log off at the end their work period, regardless of the sensitivity of information on the system. If agency business requirements necessitate a deviation, rationale and procedures shall be documented.
- Locking screensavers to be in use on all personal computers (including laptops). Screensavers shall be automatically activated by the personal computer's operating system after a specific period of inactivity. The period of inactivity shall be determined by the agency.

4.2. PASSWORD PROTECTION FOR LOCKING SCREENS**:** Requirements for password strength used on locking screen savers shall be determined by the capabilities of the applicable operating system. Passwords used to unlock screens shall meet requirements of Statewide Standard, Authentication and Directory Services S-STD-001, unless otherwise prevented by the capabilities of the applicable operating system.

4.3. LOCKOUT BASED ON UNSUCCESSFUL LOGON ATTEMPTS**:** Agencies shall establish, document, implement, and communicate a requirement for locking an account from further use following a maximum number of detected, unsuccessful login attempts. Agency password resetting procedures shall ensure that the correct account holder is requesting the reset.

4.4. ACCESS (SECURITY EVENT) LOGS**:** Access logs, if available, shall be turned on and protected from accidental or deliberate overwriting. Access logs should be proactively analyzed, correlated with other logs, and evaluated. Systems should be configured to log information locally, and the logs should be sent to a remote system. Logs should contain details of:

- Access by types of user;
- Servicing activities;
- Failed sign-on attempts;
- Error / exception conditions; and
- Sufficient information to identify individual userIDs, resources, and information accessed, access paths, and patterns of access.

Access logs shall be maintained for a period of time determined by the business needs of the agency. Agencies shall establish and document access log retention requirements. Storage and backup of access logs shall be in accordance with Statewide Backups Standard S-STD-010.

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 IT Standards

7. Attachments

None

8. Version Control

S-STD-007.002

9. Revision History

Original 4/28/05
Revised 5/05/05
Format Updated 09/18/13