STATE of ARIZONA

Government Information Technology Agency	Statewide STANDARD	TITLE: Session Controls
	P800-S825 Rev 2.0	Effective Date: October 10, 2008

1. AUTHORITY

The Government Information Technology Agency (GITA) shall develop, implement and maintain a coordinated statewide plan for information technology (IT) (A.R.S. § 41-3504(A (1))), including, the adoption of statewide technical, coordination, and security standards (A.R.S. § 41-3504(A (1(a)))).

2. PURPOSE

The purpose of this standard is to coordinate budget unit 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 budget units. Budget unit 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 Arizona Board of Regents but excluding the universities under the jurisdiction of the Arizona Board of Regents the community college districts and the legislative or judicial branches. A.R.S. § 41-3501(2).

The Budget Unit Chief Executive Officer (CEO), working in conjunction with the Budget Unit Chief Information Officer (CIO), shall be responsible for ensuring the effective implementation of Statewide Information Technology Policies, Standards, and Procedures (PSPs) within each budget unit.

4. STANDARD

The following session controls provide minimum requirements for preventing unauthorized access to information, systems, applications, and networks via unattended workstations at budget units, regardless of location, throughout the State. Requirements shall be documented and maintained as part of, and in accordance with, Statewide Standard P800-S810, Account Management.

4.1 SESSION/SYSTEM TIMEOUT**:** Budget units 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 to log off at the end of the business day, regardless of the sensitivity of information on the system. If budget unit 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 budget unit.

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 P800-S820, Authentication and Directory Services, unless otherwise prevented by the capabilities of the applicable operating system.

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

4.4 STRONG AUTHENTICATION: In controlling the authenticity of local and/or remote user identities, it is recommended that budget unit's provide at least two of the three authentication methods as identified in the Statewide Standard P800-S820 Authentication and Directory Services, authentication by knowledge, authentication by ownership, and/or authentication by characteristic.

4.5 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 budget unit. Budget units shall establish and document access log retention requirements. Storage and backup of access logs shall be in accordance with Statewide Standard P800-S870, Backups.

5 DEFINITIONS AND ABBREVIATIONS

Refer to the PSP Glossary of Terms located on the GITA website at http://www.azgita.gov/policies_standards/ for definitions and abbreviations.

6. REFERENCES

6.1. A. R. S. § 41-621 et seq., "Purchase of Insurance; coverage; limitations, exclusions; definitions."
6.2. A. R. S. § 41-1335 ((A (6 & 7))),"State Agency Information."
6.3. A. R. S. § 41-1339 (A),"Depository of State Archives."
6.4. A. R. S. § 41-1461, "Definitions."
6.5. A. R. S. § 41-1463, "Discrimination; unlawful practices; definition."
6.6. A. R. S. § 41-1492 et seq., "Prohibition of Discrimination by Public Entities."
6.7. A. R. S. § 41-2501 et seq., "Arizona Procurement Codes, Applicability."
6.8. A. R. S. § 41-3501, "Definitions."
6.9. A. R. S. § 41-3504, "Powers and Duties of the Agency."
6.10. A. R. S. § 41-3521, "Information Technology Authorization Committee; members; terms; duties; compensation; definition."
6.11. A. R. S. § 44-7041, "Governmental Electronic Records."
6.12. Arizona Administrative Code, Title 2, Chapter 7, "Department of Administration Finance Division, Purchasing Office."
6.13. Arizona Administrative Code, Title 2, Chapter 10, "Department of Administration Risk Management Section."
6.14. Arizona Administrative Code, Title 2, Chapter 18, "Government Information Technology Agency."
6.15. Statewide Policy P100, Information Technology.
6.16. Statewide Policy P800, IT Security.
    6.16.1. Statewide Standard P800-S810, Account Management.
    6.16.2. Statewide Standard P800-S820, Authentication and Directory Services.
6.17. State of Arizona Target Security Architecture, http://www.azgita.gov/enterprise_architecture.

7. ATTACHMENTS

None.