STATE of ARIZONA

Government Information Technology Agency	**Statewide STANDARD**	**TITLE: Account Management**
	P800-S810 Rev 2.0	**Effective Date: September 12, 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 implementations for controlling and managing access to IT systems, applications, 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 standards provide accountability and accounting requirements for creating and changing user accounts, authorizations, and responsibilities. In accordance with Statewide Standard P800-S890, Personnel Security, standards contained in this document shall apply to State employees and contractors.

4.1. **POLICIES AND PROCEDURES:** Budget units 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:** Budget units shall establish, document, and communicate a policy requirement that accountability for actions taken on an IT resource (e.g., computer system, budget unit 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 Statewide Standard P800-S890, Personnel Security, 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 Statewide Standard P800-S895, Security Training and Awareness.

- A non-disclosure agreement shall be signed by any State employee or contractor (see Attachment A) who requires access to sensitive information, prior to being granted access to that information. Statewide Standard P740-S741, Classification and Categorization of Data, defines confidential information requirements and provides the opportunity for budget units 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 Statewide Standard P800-S890, Personnel Security, budget units 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 budget unit, change of duties within the budget unit, resignation, termination, and report of alleged inappropriate behavior (as defined by the budget unit) by an employee.
- Events apply to budget unit 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:** Budget units 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 budget unit shall establish and document procedures to identify all holders of remote access privileges to budget unit 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 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 P740, Data/Information Architecture.
  6.16.1. Statewide Standard P740-S741, Classification and Categorization of Data.
6.17. Statewide Policy P800, IT Security.
  6.17.1. Statewide Standard P800-S890, Personnel Security.
  6.17.2. Statewide Standard P800-S895, Security Training and Awareness.
6.18. State of Arizona Target Security Architecture, http://www.azgita.gov/enterprise_architecture.

7. ATTACHMENTS

Attachment A. Sample Non-Disclosure Agreement for Access to Sensitive Information

ATTACHMENT A. SAMPLE NON-DISCLOSURE AGREEMENT FOR ACCESS TO SENSITIVE INFORMATION

Non-Disclosure Agreement for Access to Sensitive Information

Agency Name

I, _____ have read and understand the Statewide Account Management
Print Name
Standard (S810) and agree to comply with all of the terms and conditions of this standard with respect to Written Access Authorization to personal/confidential information considered sensitive by the State.

I also understand and agree that sensitive information . . .

a. shall not be digitally and/or electronically copied or manually reproduced without the express approval of a Written Access Authorization from the Agency.

b. digitally and/or electronically copied or manually reproduced shall, upon request by Agency Management, be returned to the Agency.

c. that has been breached, compromised, or stolen, be immediately reported to Agency Management.

d. shall not directly or indirectly be exploited or disclosed to any person, organization, or third party for any purpose except as described or expressly authorized by Agency Management.

e. shall be used solely for purposes of conducting business for the State and to benefit the State for better efficiencies and effectiveness in State government.

f. shall remain the property of the State and held in trust by all State employees and Contractor's when Written Access Authorization has been granted.

g. authorized for my use shall be protected through the use of encryption technologies when utilizing remote and/or mobile technologies (includes digital/electronic transactions and data repositories on storage devices).

This is a formal agreement on proper behavior for managing sensitive information by all State employees and its contractor's. All network and information systems activities conducted with State resources is the property of the State of Arizona.

Signed: _____

Date: _____

LIABILITY

Neither the State of Arizona nor the _____ make warranties of any kind,
Agency Name
express or implied, for the use of State electronic information resources. Additionally, neither the State of Arizona nor the agency indicated above is responsible for any damages, whatsoever, that employees and/or contractor's may suffer arising from or related to the use of electronic information resources.