STATE of ARIZONA

Government Information Technology Agency	**Statewide POLICY**	**TITLE: IT Security**
	P800 Rev 3.0	**Effective Date: December 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 adopting statewide technical, coordination, and IT policy and standards (A.R.S. § 41-3504(A (1(a)))).

2. PURPOSE

To establish a statewide security policy for the protection of IT assets and resources, including data/information for Budget Units with their own network infrastructure and for those that have implemented the AZNET program for network services.

3. SCOPE

This applies to all budget units. Budget unit is defined as a department, commission, board, institution or other agency of the state 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. POLICY

The State of Arizona shall securely and economically protect its business functions, including public access to appropriate information and resources, while maintaining compliance with the legal requirements established by existing Federal and State statutes pertaining to confidentiality, privacy, accessibility, availability, and integrity.

Budget Units that are maintaining their own network infrastructure shall tightly integrate its security architecture/technologies with common services including Remote Access, Internet Access, Firewall, VPN, Spam and Anti-Virus Email Filtering, and other services that comply with this policy and related IT security standards in addition to the AZNET program.

Budget Unit's that have implemented the AZNET program for network services, security architecture/technologies are specifically designed to support and

integrate tightly with a converged network that offers security for common services including Remote Access, Internet Access, Firewall, VPN, Spam, and Anti-Virus Email Filtering, and other services that comply with this policy and related IT security standards. AZNET's security program will further eliminate unauthorized third party Internet connections in addition to improving the State's network security posture through a centralized security infrastructure.

4.1. IT SECURITY POLICY RESPONSIBILITIES

The policy establishes that budget units shall:

4.1.1. Protect the State's IT assets, resources, and data/information from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide:

- Integrity, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity;
- Confidentiality, which means preserving authorized restrictions from access and disclosure, including means for protecting personal privacy and proprietary information;
- Availability, which means ensuring timely and reliable access to and use of information. Availability is securely accomplished through identification, authentication, authorization and access control;
- Accountability, which includes requirements that actions of individuals or entities can be traced to the individual or entity, non-repudiation, and security review controls and procedures; and
- Assurance, including security administration and adherence to Statewide IT security policies and standards.

4.1.2. Provide security protections commensurate with the risk and magnitude of harm resulting from unauthorized access, use, disclosure, modification to, or destruction of either 1) information collected or maintained by or on behalf of the budget unit or 2) information systems used by a budget unit or by a contractor of a budget unit or other organization on behalf of the budget unit.

4.1.3. Ensure that data/information contained in electronic transactions is protected via 1) identification, authentication, and authorization; 2) encryption; and 3) electronic signature, as necessary.

4.1.4. Provide adequate security for all information collected, processed, transmitted, stored, or disseminated in budget unit software application systems.

4.1.5. Ensure that networks, hardware systems, and software application systems operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls.

4.1.6. Apply security controls to information systems, resources, and data/information sufficient to contain risk of loss or misuse of the information to an acceptable level that supports the mission and operation of the budget unit.

4.1.7. Ensure that information security management processes are integrated with budget unit strategic and operational planning processes, including planning and implementing (see paragraph 4.6) any necessary remedial action to address IT security deficiencies.

4.1.8. Communicate applicable Statewide and budget-unit-specific IT security policies and standards to appropriate third-party organizations.

4.1.9. Establish IT security programs, including assignment of roles and responsibilities, as well as creation of any necessary procedures, adherence requirements, and monitoring controls that adhere to:

- *Statewide Policy P800, IT Security*;
- Applicable Statewide Standards for IT security; and
- Budget-unit-specific IT security policies, standards, and procedures.

Budget unit IT security programs shall be appropriate to each budget unit's operational and technology environment in order to provide a foundation for management to make informed decisions and IT investments that appropriately mitigate IT security risks to an acceptable level.

4.1.10. Identify, define, and resolve overlapping IT security roles/responsibilities between budget units and/or contractors relative to security services received from, or provided to, other budget units. Security services received from, or provided to, other budget units should be defined by an Inter-agency Service Agreement (ISA).

4.2. SECURITY ARCHITECTURE PRINCIPLES

The planning, design, and development of Security Architecture are guided by the following general principles that support the State's strategic business goals and objectives.

4.2.1. Security Architecture shall enable the State and its budget units to perform business processes electronically and deliver secure e-government services to the public.

4.2.2. Security levels applied to systems and resources shall, at a minimum, be commensurate with their value to the State and its budget units, and sufficient to contain risk to an acceptable level.

4.2.3. Security Architecture shall be based on industry-wide, open standards, where possible, and accommodate varying needs for and levels of security.

4.2.4. Security is a critical component of individual budget unit and State systems interoperability.
4.2.5. Security architecture shall accommodate varying security needs.

Supporting rationale for the above principles can be found in the *State of Arizona Target Security Architecture* document available at http://www.azgita.gov/enterprise_architecture.

4.3. SECURITY ARCHITECTURE TARGET TECHNOLOGIES
Components of the Target Security Architecture are reviewed and refreshed on a regular and scheduled basis to address major shifts in technology, as well as the emergence and adoption of new technology-related industry or open standards. Review criteria shall adhere to the lifecycle process described in *Statewide Policy P700, Enterprise Architecture*.

4.4. SECURITY ARCHITECTURE STANDARDS
Security Architecture defines common, industry-wide, open-standards-based technologies required to enable secure and efficient transaction of business, delivery of services, and communications among its citizens, the federal government, cities, counties, and local governments, as well as the private business sector. Security Architecture Standards allow the State and individual budget units to quickly respond to changes in technology, business, and information requirements without compromising the security, integrity, and performance of the enterprise and its information resources. Refer to Paragraph 6.20, Statewide Standards for Security Architecture, for further information.

4.5. IMPLEMENTATION
Arizona's EWTA has been designed to maximize current investments in technology, provide a workable transition path to targeted technologies, maintain flexibility, and to enhance interoperability and sharing. Security Architecture implementations shall adhere to implementation strategies described in *Statewide Policy P700, Enterprise Architecture*. Security Architecture shall be implemented in accordance with this policy, applicable statewide standards for security, and relevant Federal, and individual budget unit standards.

4.6. CONFORMANCE OF IT INVESTMENTS AND PROJECTS TO EA
To achieve the benefits of an enterprise-standards-based architecture, all information technology investments shall conform to the established EWTA that is designed to ensure the integrity and interoperability of information technologies for budget units. *Statewide Standard P340-S340, Project Investment Justification (PIJ),* defines conformance with the established EWTA and associated Statewide Policies and Standards. Variances from the established EWTA shall be documented and justified in the appropriate section of the PIJ document.

4.7. APPLICABILITY TO OTHER STATEWIDE EA POLICIES AND STANDARDS

Statewide Policy P800, IT Security, adheres to and demonstrates the purpose established in *Statewide Policy P100, Information Technology*. *Statewide Policy P800, IT Security*, adheres to the principles, governance, lifecycle process, and implementation elements described in *Statewide Policy P700, Enterprise Architecture*.

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. Federal Office of Management and Budget (OMB) Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources."
6.16. State of Arizona Target Security Architecture.
6.17. Statewide Policy P100, Information Technology.
6.18. Statewide Policy P340, Project Investment Justification (PIJ).
  6.18.1. Statewide Standard P340-S340, Project Investment Justification.
6.19. Statewide Policy P700, Enterprise Architecture.
6.20. Statewide Policy P800, IT Security.
  6.20.1. Statewide Standard P800-S805, IT Risk Management.
  6.20.2. Statewide Standard P800-S810, Account Management.
  6.20.3. Statewide Standard P800-S815, Configuration Management.
  6.20.4. Statewide Standard P800-S820, Authentication and Directory Services.

6.20.5. Statewide Standard P800-S825, Session Controls.
6.20.6. Statewide Standard P800-S830, Network Infrastructure.
6.20.7. Statewide Standard P800-S850, Encryption Technologies.
6.20.8. Statewide Standard P800-S855, Incident Response and Reporting.
6.20.9. Statewide Standard P800-S860, Virus and Malicious Code Protection.
6.20.10. Statewide Standard P800-S865, IT Disaster Recovery Planning (DRP).
6.20.11. Statewide Standard P800-S870, Backups.
6.20.12. Statewide Standard P800-S875, Maintenance.
6.20.13. Statewide Standard P800-S880, Media Sanitizing/Disposal.
6.20.14. Statewide Standard P800-S885, IT Physical Security.
6.20.15. Statewide Standard P800-S890, Personnel Security.
6.20.16. Statewide Standard P800-S895, Security Training and Awareness.

7. ATTACHMENTS

None.