

STATE of ARIZONA

Arizona Department Of Administration	<b>Agency STANDARD</b> A800-M1-S01                      Rev. 0	TITLE: <u>ADOA Information Security Program</u>  Effective Date: January 31, 2009
---	---	---

**1. AUTHORITY**

- 1.1. The authority for this Standard is based on Arizona Revised Statute 41-703 and the ADOA Policy A800 – Information Security Policy.

**2. PURPOSE**

- 2.1. The purpose of this Standard is to establish the responsibilities and restrictions to be complied with by all users of ADOA Information Resources.

**3. SCOPE**

- 3.1. This Standard applies to all ADOA employees, contractors and other entities using ADOA Information Resources.
- 3.2. The ADOA Director, in conjunction with the ADOA Chief Information Officer (CIO) and the ADOA Information Security (AIS) Manager, is responsible for ensuring the effective implementation of ADOA Information Security Policy and Standards which reference the Statewide Information Technology Policies and Standards.

**4. DEFINITIONS AND ABBREVIATIONS**

- 4.1. **ADOA** – Arizona Department of Administration
- 4.2. **AIS** - ADOA Information Security
- 4.3. **AIS Manager** – ADOA Information Security Manager
- 4.4. **Information Resources** - any computing device, peripheral, software, local and wide area networks (LAN and WAN), communications equipment (including Fax machines and telephones), communications software (including the Internet, Intranet, and bulletin board access software), Virtual Private Network (VPN) or remote access capabilities and data distribution, electronic data or related consumable (e.g. paper, disk space, central processor time, network bandwidth) information and data owned or controlled by the ADOA.
- 4.2. **Information Security** - The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
- 4.3. **Information System** - A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
- 4.4. **Information Technology** - Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage,

manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.

- 4.5. **Management Controls** - The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security.

**Operational Controls** - The security controls (i.e., safeguards or countermeasures) for an information system that primarily are implemented and executed by people (as opposed to systems).

- 4.6. **Risk** - The level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.
- 4.7. **Risk Management** - The process of managing risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system. It includes risk assessment; cost-benefit analysis; the selection, implementation, and assessment of security controls; and the formal authorization to operate the system. The process considers effectiveness, efficiency, and constraints due to laws, directives, policies, or regulations.
- 4.8. **Safeguards** - Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.
- 4.9. **Security Category** - The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals.
- 4.10. **Security Controls** - The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

- 
- 4.11. **Security Control Baseline** - The set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system.
  - 4.12. **Security Control Enhancements** - Statements of security capability to:
    - (i) build in additional, but related, functionality to a basic control; and/or
    - (ii) increase the strength of a basic control.
  - 4.13. **Technical Controls** - The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.
  - 4.14. **Threat** - Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
  - 4.15. **User** - Individual or (system) process authorized to access an information system.
  - 4.16. **Vulnerability** - Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
  - 4.17. **Vulnerability Assessment** - Formal description and evaluation of the vulnerabilities in an information system.
- 5. STANDARD**
- 5.1 The ADOA Information Security (AIS) Manager shall develop, implement and administer an ADOA Information Security Program. The program shall ensure ADOA's compliance with U.S. and State, laws, codes, rules, regulations regarding the secure protection of ADOA information resources.
  - 5.2 The ADOA Information Security Program shall consist of the following:
    - A. Policy
    - B. Standards
    - C. Procedures
    - D. Security Awareness Training
    - E. Internal Security Assessments
    - F. External Security Assessments & Audits
    - G. Management Reporting
  - 5.3 **Policy** – The ADOA Information Security Policy, A-800, is for the implementation and maintenance of information security controls that

protect ADOA information resources. This policy shall ensure preservation of the confidentiality, integrity and availability of information resources that are under the responsibility of the Arizona Department of Administration.

- 5.4. **Standards** – The ADOA Information Security Standards will detail the minimum acceptable allowed controls for the protection of ADOA information resources. These standards are based on NIST SP 800-53 and Arizona Statewide Policy and Standards. They consist of the following recommended security control groups and controls:

**A. Management**

- 5.4.A.1. Information Security Program
- 5.4.A.2. Risk Assessment
- 5.4.A.3. Security Planning
- 5.4.A.4. Asset Acquisition, Implementation and Disposal
- 5.4.A.5. Certification, Accreditation, & Security Assessment

**B. Operational**

- 5.4.B.1. Personnel Security
- 5.4.B.2. Physical & Environmental Protection
- 5.4.B.3. Contingency Planning
- 5.4.B.4. Configuration Management
- 5.4.B.5. System Maintenance
- 5.4.B.6. System & Information Integrity
- 5.4.B.7. Media Protection
- 5.4.B.8. Security Awareness & Training
- 5.4.B.9. Incident Response

**C. Technical**

- 5.4.C.1. Identification & Authentication
- 5.4.C.2. Access Control
- 5.4.C.3. Audit & Accountability
- 5.4.C.4. System & Communications

- 5.5. **Procedures** – The ADOA Information Security Procedures detail the exact step-by-step method of performing a particular process in relation to the ADOA Information Security Standards.

- 5.6. **Security Awareness Training** – The ADOA Information Security Awareness Training Program educates the users of the ADOA information

resources of security best practices to help protect the confidentiality, integrity and availability of those resources.

- 5.7. **Internal Security Assessments** – The ADOA Information Security Standard, A800-M2-S03 – Vulnerability Scanning, Section 5.1, states that network and host vulnerability scanners are used to test for the vulnerabilities of internal system and network perimeter defenses. Scanning for vulnerabilities allows AIS to measure and manage risk by identifying and eliminating security vulnerabilities, providing a more secure network environment.

Review of the security controls in each system shall be performed when significant modifications are made to the system or at least every 30 days to assure that management, operational and technical controls are functioning effectively. Penetration testing of the network and host devices will be performed annually. The scope and frequency of the review should coincide with the acceptable level of risk for the system.

- 5.8. **External Security Assessments & Audits** – The ADOA Information Security Standard A800-M2-S03 – Vulnerability Scanning, Section 5.3, states that an independent external audit shall be performed at least every three years to assess the security controls for the ADOA network infrastructure host systems and each major application.
- 5.9. **Management Reporting** – The ADOA Information Security reporting will be used to inform management of the current state of security controls for ADOA information resources and help identify non-compliance and address the need for further controls or the modification of current controls surrounding those resources.

## **6. STANDARD NON-COMPLIANCE**

- 6.1. All departments owning ADOA Information Resources are responsible for understanding and adhering to this Standard.
- 6.2. For non-compliance with this Standard, all ADOA employees shall be subject to Human Resource progressive discipline up to and including dismissal, with the exception that management may choose to take appropriate action commensurate with the seriousness of the offense. In addition, any non-compliance with this Standard that may constitute a violation of State or Federal criminal statute may be referred to a law enforcement agency for appropriate action.
- 6.3. Contractors and other authorized users will be held to contractual agreements. In addition, any non-compliance with this Standard that may constitute a violation of State or Federal criminal statute may be referred to a law enforcement agency for appropriate action.

## **7. REFERENCES**

- 7.1. Statewide Policy – P800, IT Security
- 7.2. ADOA Policy A800 – Information Security

- 7.3. National Institute of Standards and Technology Special Publication 800-53 Recommended Security Controls for Federal Information Systems, February 2005.

**8. ATTACHMENTS**

None.