STATE of ARIZONA

Arizona Department Of Administration	Agency **STANDARD** A800-T4-S09 Rev 0	TITLE: **Security of ADOA Publicly Accessible Web Site Content** Effective: February 15, 2008

1. AUTHORITY

1.1. The authority for this standard is based on the ADOA Policy A800 – IT Security.

1.2. Authority flows from the applicable Statewide Policies and Standards prepared by the Government Information Technology Agency (GITA).

2. PURPOSE

2.1. The purpose of this standard is to establish requirements for controlling and approving content published on the ADOA Publicly accessible Web site.

2.2. This standard recognizes ADOA Information Security's (AIS) use of the Technology Infrastructure and Standards Assessment (TISA) as the instrument for determining compliance to ADOA and Statewide IT Policies and Standards

3. SCOPE

3.1. This standard applies to all ADOA agency business units, including divisions, contractors or other entities using agency information technology resources and data.

3.2. The ADOA Director, in conjunction with the ADOA Chief Information Officer (CIO), is responsible for ensuring the effective implementation of ADOA Information Security Policy and Standards which reference the Statewide Information Technology Policies, Standards and Procedures (PSPs).

4. DEFINITIONS AND ABBREVIATIONS

4.1. None

5. STANDARD

5.1. ADOA Business Units shall take steps to ensure that only properly approved content is published on ADOA Web sites and that content has been properly reviewed according to applicable Federal and State guidelines for privacy and security.

5.2. Some generally accepted examples of what should not be published or at least should be carefully examined and reviewed before publication on ADOA publicly accessible Web sites include the following and any combination thereof, but are not limited to:

5.2.4. Personal Information including:

5.2.4.1. Name

5.2.4.2. Personal E-mail address

5.2.4.3. Home mailing address

5.2.4.4. Personal Telephone number
5.2.4.5. Social Security Numbers (SSN)
5.2.4.6. Medical records
5.2.4.7. Personal financial information.
5.2.4.8. Detailed biographical material (could be employed for social engineering)
5.2.4.9. Staff family members

5.2.5. Designated classified, sensitive or proprietary information and records.
5.2.6. Information on the composition or preparation of hazardous materials or toxins.
5.2.7. Sensitive information relating to homeland security
5.2.8. An organization's detailed physical and information security safeguards.
5.2.9. Details about an organization's network and information system infrastructure (e.g., address ranges, naming conventions, access numbers).
5.2.10. Information that specifies or implies physical security vulnerabilities.
5.2.11. Detailed plans, maps, diagrams, aerial photographs, and architectural drawings of organizational buildings, properties, or installations.
5.2.12. Internal personnel rules and procedures.
5.2.13. Telephone numbers, e-mail addresses, or general listings of staff unless necessary to fulfill organizational requirements.
5.2.14. Schedules of agency personnel or their exact location (whether on or off the premises).
5.2.15. Investigative records.
5.2.16. Organization's physical and information security procedures
5.2.17. Information about organization's network and information system infrastructure (e.g. address ranges, naming conventions, access numbers).
5.2.18. Information that specifies or implies physical security vulnerabilities.
5.2.19. Information on disaster recovery or continuity of operations plans except as absolutely required.
5.2.20. Details on emergency response procedures, evacuation routes, or organizational personnel responsible for these issues.
5.2.21. Copyrighted material without the written permission of the owner
5.2.22. Privacy or security policies that indicate the types of security measures in place to the degree that they may be useful to an attacker.

5.3. Approval Process

5.3.4. The Director of ADOA or their representative shall be responsible for approving the information content to be published on the ADOA Web site.

5.3.5. The ADOA Chief Information Officer (CIO) or their representative shall be responsible for approving the design and functionality of the ADOA Web site.

5.3.6. ADOA Assistant Directors in charge of their respective Divisions shall be responsible for determining and approving the information to be published on their Division Web pages.

6. STANDARD NON-COMPLIANCE

6.1. All authorized users of 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, with the understood exception, that management may choose to take appropriate action commensurate with the seriousness of the offense.

6.3. Contractors and other authorized users will be held to contractual agreements.

7. REFERENCES

7.1. ADOA Policy – A800, Information Security
7.2. Statewide Policy – P800, IT Security
7.3. Statewide Policy – P170, Privacy Policy

8. ATTACHMENTS

8.1. No attachments accompany this standard.