

Arizona Department Of Administration	Agency POLICY A800-M3-S06 Rev 0	TITLE: ADOA Email Policy Effective Date: May 2, 2011
---	--	---

1. **AUTHORITY**

The authority for this policy is based on the ADOA Policy P800 – Information Security.

2. **PURPOSE**

The purpose of this policy is to establish the responsibilities and restrictions with which all users of ADOA email system must comply.

3. **SCOPE**

This policy applies to all authorized users of the ADOA email system.

4. **DEFINITIONS AND ABBREVIATIONS**

4.1. **Authorized Users:** all individuals approved to use ADOA information resources and data. These include full/part-time ADOA employees, temporary employees, contract employees and non-employees providing services or products to the agency and/or non-employees who are given access to information resources, information and data (e.g. suppliers on contract, interns or outside organizations) with intergovernmental service agreements (ISAs).

4.2. **ADOA Business Units (Business Units):** all ADOA divisions, sections, work units or other entities including non-ADOA agencies, boards and commissions using ADOA information resources.

4.3. **ADOA Business Unit Heads:** ADOA Assistant Directors, heads of sections, work units or other entities including non-ADOA agencies and persons serving as the responsible party for conducting business on behalf of ADOA.

4.4. **ADOA Email System:** ADOA Information Resource that is an electronic means for communication in which (a) text and/or attachment(s) are transmitted, (b) operations include sending, storing, processing, and receiving information, (c) users are allowed to communicate under specific conditions, and (d) messages are held in storage unit called for by the addressee

4.5. **ADOA Information Security (AIS) Manager:** the ADOA Senior Agency Information Security Officer and ADOA Agency HIPAA Security Officer. The AIS Manager reports to the ADOA Chief Information Officer and manages the Agency work group that develops, implements and enforces the ADOA Agency Information Security policies, standards, procedures and guidelines for the confidentiality, privacy, accessibility, availability, and integrity of ADOA Agency information resources. The AIS Manager directs the AIS group, which is organized to provide information security provisioning, compliance, assessment and computer investigative support for ADOA divisions and all authorized users of ADOA information resources.

- 4.6. **Attachment:** a file, such as a document, spreadsheet, or image that is sent along with an email.
- 4.7. **Business Sensitive Information:** data whose loss, corruption or unauthorized disclosure would have a significant impact to the operation of ADOA.
- 4.8. **Confidential Information:** data whose loss, corruption or unauthorized disclosure would be a violation of law or Arizona/federal mandates, policy, rule and regulations
- 4.9. **Information Resource:** 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.

5. RESPONSIBILITIES

Adherence to this policy and related standards, guidelines and procedures it encompasses is the responsibility of the following people, groups or entities:

Authorized Users of ADOA Information Resources:

- 5.1. Are responsible for complying fully with all applicable Federal, State and local laws, codes, rules, regulations, and policies.
- 5.2. Understand that access to any ADOA information resources constitutes their acknowledgement and acceptance of ADOA and Statewide policies, standards, guidelines and procedures, as well as software license agreements for software products used
- 5.3. Understand that their use of ADOA information resources has no expectation of privacy in the use of these resources or any content therein
- 5.4. Are responsible for following the restrictions on use of any ADOA information resource accessed or interfaced. This can include outside software license restrictions.
- 5.5. Shall immediately report any known violations of this policy.

ADOA Business Unit (ADOA Business Unit Head):

- 5.6. Are responsible for ensuring that their employees receive the proper training and guidance to comply with all applicable Federal and State codes, rules, regulations, and ADOA policies, standards, guidelines and procedures.
- 5.7. Shall provide assistance to the AIS Manager in monitoring the Business Unit's use of ADOA information resources without prior notice or warning to any user

- 5.8. Shall authorize the AIS Manager's requests to access the Business Unit's ADOA information resources at any time to ensure compliance with this policy.
- 5.9. May request to the Director, Deputy Director, ADOA General Counsel or ADOA HR that an investigation of improper use of ADOA information resources be initiated.
- 5.10. Shall initiate the appropriate disciplinary action to respond to violations of this policy.

ADOA Director, Deputy Director, General Counsel, or Human Resources Division:

- 5.11. Are independently authorized to instruct AIS to initiate an investigation of improper use of ADOA information resources.

ADOA Human Resources Division:

- 5.12. Is responsible for working with the ADOA Business Unit Head in evaluating and implementing the appropriate disciplinary action to respond to violations of this policy.

6. POLICY

This policy establishes the following:

- 6.1. ADOA authorized users have access to or receive a copy of this policy and *ADOA Acceptable Use of ADOA Information Resources A800-M3-S02*, which acknowledges that any abuse of an ADOA Information Resource may be cause for discipline and or dismissal. This policy applies to all authorized users.
- 6.2. ADOA reserves the right to monitor and log email use by authorized users, without notice.
- 6.3. ADOA owns all email communications and file attachments created or received in the course of State business that resides on any ADOA system. Business related messages created on non-state systems may be forwarded, carbon copied or blind copied to the creator's state email system.
- 6.4. Email records and respective attachments, whether in electronic or printed form, if required to be retained, preserved and/or disposed of in accordance with public records statutes or Arizona State Library, Archives and Public Records requirements, should be handled as required (A.R.S. § 41-1335, A.R.S. § 41-1339, A.R.S. § 41-1348, A.R.S. § 41-1350 & A.R.S. § 44-7041).
- 6.5. System-generated message content such as: auto-reply rules, out-of-office alerts, and signatures blocks shall be approved by ADOA Business Unit Heads.

This policy further establishes that an ADOA authorized user shall not:

- 6.6. Share email account information, except for an employee's assistant having access to his/her supervisor's email, user logon IDs or passwords.

- 6.7. Intercept or attempt to intercept any email messages a user is not authorized or intended to receive.
- 6.8. Use unauthorized anonymous and pseudonymous addresses for sending/receiving emails.
- 6.9. Modify or delete email messages or files from within another individual's email account, with maliciousness or intent to deceive
- 6.10. Alter the content of an email message originating from another person or computer, with maliciousness or intent to deceive.
- 6.11. Misrepresent or forge the identity of the sender or the source of an email message.
- 6.12. Send/forward email messages using another person's email account unless delegated rights are granted and documented.
- 6.13. Auto-forward email messages to an external mail account(s) outside of control of ADOA without prior written approval of the Director or Deputy Director
- 6.14. Intentionally or in a grossly negligent manner leading to the disruption of or damage to ADOA's email system(s) and its information.
- 6.15. Include verbiage or taglines in system-generated auto-reply rules, out-of-office alerts, and signatures, or add taglines generally to any ADOA generated e-mails. A tagline is a quote or saying usually (but not necessarily) added at the end of an e-mail under the name of the person sending the e-mail that makes a point. These items will not be allowed unless related to business purposes and approved in writing by the employee's Assistant Director and Director or Deputy Director.
- 6.16. Knowingly send/forward or initiate receipt of email that:
 - A. Disrupts, obstructs or burdens network resources for non-business purposes (i.e., chain letters, junk mail);
 - B. Contains Confidential or Business Sensitive data, unless it is in the course of State Business and meets Federal and State agency privacy/security requirements (HIPAA Privacy Rule 45 CFR Parts 160 and 164, Statewide Privacy Policy P170, ADOA Standard A800-M02-S02);
 - C. Utilizes email for any illegal purpose;
 - D. Conducts any gambling, betting or gaming activity;
 - E. Conducts any solicitation activity, except as identified by A.A.C. R2-11-309A;
 - F. Promotes special events other than as approved by Arizona Department of Administration Office of Special Events in accordance with A.A.C. R2-11-401 through R2-11-409, or as approved by the ADOA Ombudsman;
 - G. Violates or infringes on the rights of any other person;
 - H. Contains nudity, defamatory, false, abusive, obscene, pornographic, profane, sexually-oriented, threatening, racially-offensive or otherwise biased, discriminatory or illegal material from state systems or in the course of conducting state business from personal accounts accessed or utilized by the

employee (i.e. Hotmail, Yahoo, or any web mail provided by the employee's Internet Service Provider); or

I. Violates any applicable Federal, State or local laws and regulations.

7. **POLICY NON-COMPLIANCE**

7.1. All authorized users of the ADOA email system are responsible for understanding and adhering to this policy.

7.2. An ADOA employee who is found in non-compliance with this policy shall be subject to discipline up to and including dismissal. In addition, any non-compliance with this policy that may constitute a violation of a Federal, State or Municipal criminal statute may be referred to a law enforcement agency for appropriate action.

7.3. Contractors and other authorized users will be held to contractual agreements. In addition, any non-compliance with this policy that may constitute a violation of a State or Federal criminal statute may be referred to a law enforcement agency for appropriate action.

8 **REFERENCES:**

- 8.1. HIPAA Privacy Rule 45 CFR Parts 160 and 164
- 8.2. A.R.S. § 41-770
- 8.3. A.R.S. § 41-703
- 8.4. A.R.S. § 41-1346 (8)
- 8.5. A.R.S. §41-1350
- 8.6. A.R.S. § 41-1351
- 8.7. Statewide Policy P170, Privacy
- 8.8. ADOA Policy A800, IT Security
- 8.9. ADOA Standard A800-M02-S02, Data Classification and System Categorization
- 8.10. ADOA Standard A800-M2-S03, Risk Management

9. **ATTACHMENTS:** None

10. **APPROVAL**

Approved by:



Scott A. Smith
Director

5/2/11
Approval Date