CHAPTER: 100

Agency Administration/Management

DEPARTMENT ORDER:

102 – Information Technology

OFFICE OF PRIMARY RESPONSIBILITY:

DD

Effective Date:

February 10, 2021

Amendment:

N/A

Supersedes:

DO 102 (2/11/17)

Scheduled Review Date:

January 1, 2024

ACCESS

☐ **Contains Restricted Section(s)**

Arizona Department of Corrections Rehabilitation and Reentry

Department Order Manual

FOR

David Shinn, Director

TABLE OF CONTENTS

STANDARDS

American Correctional Association (ACA) Standards: 5-ACI-1F-01, 5-ACI-1F-02, 5-ACI-1F-03, 5-ACI-1F-04, 5-ACI-1F-05, 5-ACI-1F-06, and 5-ACI-1F-07

PURPOSE

This Department Order establishes standards for the development and integration of efficient, cost-effective information systems to support the Arizona Department of Corrections, Rehabilitation and Reentry (Department) mission and goals. All information systems shall adhere to these standards and be implemented through the processes established by this Department Order. All information technology investments made within the Department shall meet minimum performance standards and criteria outlined in the Department Order.

APPLICABILITY

This Department Order does not apply to computer systems owned by private corporations operating private prison facilities. Information systems operated by private prison facilities shall be governed by contract where it is necessary for the private computer system to interface with Department systems.

PROCEDURES

1.0 GENERAL RESPONSIBILITIES

1.1 All employees shall protect data stored on computers, laptops or any electronic device from unauthorized access in accordance with the Statewide Access Agreement, F8280. No data shall be removed from Department electronic devices without the written consent of the Inspector General.

1.2 Human Resources or designee shall notify Information Technology (IT) when an employee retires or terminates employment. {5-ACI-1F-06}

1.3 The Department's Executive Team shall approve, deny, revise, prioritize or take other appropriate action on IT projects related to Department strategy.

1.4 The Department's Chief Information Officer (CIO) shall: {5-ACI-1F-04}

1.4.1 Annually review this Department Order, update as necessary, and communicate to all staff. {5-ACI-1F-04} {5-ACI-1F-05}

1.4.2 Periodically review and revise Department standards for hardware and software as outlined in this Department Order.

1.4.3 Review requests for new equipment and systems for compliance with the Department's Five Year Strategic Plan and Department policy and procedures.

1.4.4 Coordinate activities related to computer and telecommunications hardware and software systems such as:

1.4.4.1 Designing and installing systems.

1.4.4.2 Maintaining and repairing computers, peripheral and telecommunications equipment.

1.4.4.3 Ensuring the security of hardware, software, networks and storage.

1.4.5 Collaborate with institutions and bureaus when planning system expansions, including:

1.4.5.1 Transfer and control of equipment and software.

1.4.5.2 Changes in the function of computer and telecommunications hardware and software systems.

1.4.6 Provide analysis, input, and recommendations to staff regarding their automation requirements.

1.4.7 Approve or deny requests for exceptions to current standards depending on the specific application and need.

1.4.8 Review statewide software applications and requirements, and provide recommendations to the Executive Team.

1.4.9 Install and maintain data management systems to collect, store, retrieve and process essential information regarding: {5-ACI-1F-01}

1.4.9.1 The network infrastructure linking all Department locations to the Arizona Department of Administration (ADOA) data center, and other external agencies.

1.4.9.2 Other network-based applications residing on any Departmental Local Area Network (LAN) and/or Wide Area Network (WAN) server(s).

1.4.10 Provide information about automated technology plans and system capabilities to the Director, Deputy Directors, and Assistant Directors.

1.4.11 Serve as the Department's representative in programs and projects involving information management issues, including the development of appropriate written instructions.

1.4.12 Employ formal project management techniques in the planning, design, development, implementation, and maintenance of IT projects and functions.

1.4.13 Develop, administer and monitor compliance with the provisions of the Department's IT Strategic Plan through the Planning Application for Reporting IT Strategies (PARIS) submitted annually, during the budgeting process, to the ADOA/Arizona Strategic Enterprise Technology (ASET) Office.

1.5 Wardens, Deputy Wardens, Bureau Administrators, Administrators, Contract Beds Bureau Monitors and contractors who are authorized to possess or are using Department computing devices shall ensure inmates do not have access to those devices, removable storage devices or printers, unless specifically authorized. {5-ACI-1F-05}

1.6 Inmates may be granted access to computer systems which are secured and locked down via Group Policy to allow them access to only the applications in which they are required to work. These end points shall be on a designated inmate network which does not have access to the Department staff production data and the Internet. {5-ACI-1F-05}

1.6.1 Controlled access to the internet may be permitted in qualifying instances. This includes, but may not be limited to: education and work programs.

1.7 Training {5-ACI-1F-07}

1.7.1 All employees shall be required as part of their annual training requirement to take the "Information Technology and Security Awareness" Computer Based Training course. (See Department Order #509, Employee Training and Education.) Failure to complete the required training, may result in account suspension.

1.7.1.1 All contractors who are authorized to possess or are using any Department computing device shall be required as part of their contractual agreement to ensure all staff on Department properties have taken and completed the "Information Technology and Security Awareness" Computer Based Training course.

1.7.2 Staff Development and Training Bureau shall track security awareness training and education compliance for all employees and contractors with access to Department information systems, which include periodic refresher training and education.

1.7.2.1 A complete training report shall be sent to the Information Security Office monthly. This report shall include:

1.7.2.1.1 Trainees Full Name

1.7.2.1.2 Training Course Name

1.7.2.1.3 Completion Status

1.7.2.1.4 Completion Date

1.8 Employees shall ensure possession of personal telephonic communication equipment is in accordance with Department Order #513, Employee Property, and it shall not be connected to the Department infrastructure.

1.9 Department staff may only use Department issued mobile devices that are password protected within the secure perimeters of the institution, in accordance with Department Order #104, Communications System.

1.9.1 All Department issued cellular devices shall maintain Mobile Device Management (MDM) software at all times.

1.9.2 All laptops and cellular devices must be encrypted with the Department approved security software.

1.9.3 The Department's IT must be notified immediately if a Department issued mobile device is lost or stolen.

1.9.4 All Department issued laptops and tablets must be secured with Department approved security software.

1.10 Supervisors shall ensure all employees and contractors who require access to personal and/or confidential information complete and sign a Non-Disclosure Agreement for Access to Sensitive Information, Form 102-3, prior to being given access to information and distributed as indicated on the form. {5-ACI-1F-02} {5-ACI-1F-07}

2.0 AUTOMATED OFFICE SYSTEMS - EMAIL AND MESSAGING {5-ACI-1F-06}

2.1 The use of automated office systems shall be in accordance with the ASET Email Policy P401. For current information, access ASET policy located at (https://aset.az.gov/).

2.1.1 Employees shall only use the Department's automated office systems for official business and for approved solicitation requests.

2.1.2 A solicitation request is allowed only if the request has been submitted and approved in accordance with Department Order #111, Solicitation.

2.1.3 All documents created in the automated office systems are considered public records, unless they have been deemed attorney client communication by the Department's General Counsel or the Attorney General's Office.

2.1.4 The professional standards apply to Department memorandums, in terms of subject and vocabulary shall be applied to automated office system communications. (See Department Order #103, Correspondence/Records Control.)

2.1.5 Emails shall contain a proper "Complimentary Close."

2.1.5.1 A complimentary close is the part of a letter which by convention immediately precedes the signature or ending name block for unsigned correspondences. Complimentary closings shall be used carefully and shall be professional and appropriate for the situation.

2.1.5.2 Proper complimentary closing shall include any of the following:

2.1.5.2.1 Sincerely

2.1.5.2.2 Regards

2.1.5.2.3 Respectfully

2.1.5.2.4 No complimentary closing (Some instances do not call for a complimentary closing.)

2.1.5.3 Email signatures shall only contain name, title and contact information. No quotes, sayings or other items are permitted.

2.1.6 Employees shall ensure emails contain the following information: This email contains information that is intended only for the person(s) to whom it is addressed. If you received this communication in error, please do not retain it or distribute it and notify the sender immediately.

2.2 Initial Set-Up and Upgrades

2.2.1 The Department's IT shall maintain the email system, software and standards for the Department.

2.2.2 New installations or upgrades to the automated office system shall be coordinated through and approved by the CIO or an appropriate designee.

2.3 Email Access

2.3.1 Authorized employees may be granted an email account based on job function. {5-ACI-1F-07}

2.3.2 Temporary, short-term and contract employees shall be assigned an email address upon request from the approving authority.

2.3.3 Automated office system software may be installed on "shared use" or shift computers used for work upon request from the appropriate approving authority.

2.3.4 A Department email client, program or capability shall not be installed on a computer to which inmates have access.

2.4 Broadcast Emails – Broadcast emails are a general message which is sent to a large number of users or an entire staff distribution group.

2.4.1 Users wishing to send a broadcast message shall receive prior written authorization from the appropriate approving authorities. Examples: A user wishing to send a broadcast message to a bureau shall obtain prior authorization from the Bureau Administrator. A user wishing to send a broadcast message to the Department shall obtain prior authorization from the Director.

2.4.2 Approved broadcast emails with an attachment of greater than 25 Megabyte (MB), or whenever possible for smaller size attachments, shall be sent as a link.

2.5 Delegate Rights

2.5.1 Individuals may give access to their mailbox to co-workers. In addition, staff may share email folders and calendars with co-workers which may need access to the information.

2.5.2 Delegate access rights may include reading and writing to documents or may be limited to read only. Typically, access rights shall be limited to "read only." Discretion shall be used in assigning "write permissions" since the action of the delegate, in such cases, cannot be distinguished from the grantor and is the responsibility of the grantor.

2.6 Email Search Requests

2.6.1 When initiating an email search request, the requestor shall complete the Email Search Request, Form 102-2, and forward the form through their chain of command to the appropriate approving authority. The request shall include the following information:

2.6.1.1 Reason for the request

2.6.1.2 Case number(s), if applicable

2.6.1.3 Custodian(s) whose emails are the subject of the search

2.6.1.4 Searchable "key" words

2.6.1.5 Specific dates of inquiry

2.6.2 Authorized email search requests may only be approved by one of the following:

2.6.2.1 Director

2.6.2.2 Deputy Director

2.6.2.3 General Counsel

2.6.2.4 Inspector General

2.6.3 Approved Email Search Request forms shall be scanned via email by the requestor to the E-discovery staff at Ediscovery@azadc.gov, and shall not be sent to individual staff members email accounts.

2.6.3.1 The E-discovery staff shall not commence the work requests until after the approval has been granted by the approving authority.

2.6.4 Upon receipt of the request(s) the E-discovery staff shall:

2.6.4.1 Reply to the requestor confirming the receipt of the request and identifying the individual staff member who will be conducting the search.

2.6.4.2 Enter and record the information outlined in 2.6.4.2.1 through 2.6.4.2.10 of this section, in the respective E-discovery Logs (i.e., Litigation, Administrative Investigations Unit, Equal Employment Opportunity, and the Public Records logs). The E-discovery Logs shall include the following information:

2.6.4.2.1 Requestor

2.6.4.2.2 External Requestor (public records request) – The individual(s) full name, agency, department, and corporation (example, Channel 12 News).

2.6.4.2.3 Date of request(s) received from external or internal requestor

2.6.4.2.4 Case number(s), if applicable

2.6.4.2.5 Custodian(s) whose emails are the subject of the search

2.6.4.2.6 Approving authority

2.6.4.2.7 Date of approval

2.6.4.2.8 Date request received by E-discovery staff

2.6.4.2.9 E-discovery delivery date – The date the requested data was delivered to the requestor.

2.6.4.2.10 E-discovery delivery receipt – The person the data was delivered to.

2.7 Upon completion of the requested search, the E-discovery staff shall forward the requested data to the requestor, absent additional instructions by the approving authority, listed on the Email Search Request form.

2.8 The Inspections Unit shall conduct periodic internal inspections in accordance with Department Order #606, Internal Inspections Programs.

2.9 Internet Browsing History Requests

2.9.1 When initiating an internet browsing history request, the requester shall complete the Internet Browsing History Request, Form 102-7, and forward the form through their chain of command to the appropriate approving authority. The request shall include the following information:

2.9.1.1 Reason for request

2.9.1.2 Case number(s), if applicable

2.9.1.3 User whose internet browsing history is to be reviewed

2.9.1.4 Computer where the internet browsing occurred

2.9.1.5 Searchable keywords or websites

2.9.1.6 Specific dates of inquiry

2.9.2 Authorized internet browsing requests may only be approved by one of the following:

2.9.2.1 Director

2.9.2.2 Deputy Director

2.9.2.3 General Counsel

2.9.2.4 Inspector General

2.9.3 Approved Internet Browsing History Request forms shall be uploaded into the IT Ticketing System, and shall not be sent to individual IT staff members email accounts.

2.9.3.1 IT staff shall not commence the work request until after the approval has been granted by the approving authority.

2.9.4 Upon receipt of the request(s) the IT staff shall:

2.9.4.1 Reply to the requestor confirming the receipt of the request and identifying the individual IT staff member who will be conducting the search.

2.9.4.2 Verify that the request is properly formed and approved. If the request is missing information, IT will request clarification from the requester.

2.9.4.3 Obtain all available internet browsing history that matches the requested criteria from the following:

2.9.4.3.1 The indicated computer

2.9.4.3.2 The Department's firewall

2.9.4.3.3 Any other sources available

2.9.4.4 Attach any internet browsing history to the request inside the IT Ticketing System, provide the internet browsing history to the requester, and close the request.

3.0 LAN/WAN HARDWARE AND NETWORK INFRASTRUCTURE – All acquisitions of hardware, and network infrastructure components and equipment, shall meet the criteria, be reviewed and approved as outlined in section 5.0.

4.0 IT SUPPORT PROCEDURES - The Service Ticket process shall be used to address basic operational problems with existing systems, relating to repairing or restoring current functionality, and also includes requests for enhancements, modifications or the development of applications.

4.1 All tickets shall contain a detailed description of the business needs to be addressed.

4.1.1 If a ticket does not contain a detailed description of the business needs to be addressed, there may be a delay in the completion of the ticket until sufficient detail has been obtained.

4.2 The IT response time to any ticket may vary based on the ticket type, severity, and the support team assigned.

5.0 REQUESTS FOR WORKSTATION, LAN/WAN HARDWARE, SOFTWARE AND MOBILE DEVICES

5.1 All requests for acquiring new technology shall comply with Department Order #302, Contracts and Procurement.

5.2 All projects shall comply with the ASET policy.

5.2.1 Projects over $25,000 require a Project Investment Justification. IT shall coordinate development of the Project Investment Justification document for approval by the Director and submission to the ADOA/ASET Office for their review and approval. A Project Investment Justification approval letter from ASET shall accompany all purchase order**s** (PO's) sent to the Procurement Officer.

5.2.2 Once the project is approved by ASET or Information Technology Approval Committee, the Assistant Director responsible for submitting the proposal shall appoint staff to assist IT until the project is implemented.

5.2.3 The IT Project Manager shall work in conjunction with appointed staff, outside vendors, and consultants to complete the project and shall submit monthly progress reports to the CIO through the final implementation of the project. The CIO shall brief the Executive Team during regularly scheduled meetings. IT shall also submit any periodic reports related to the project required by ASET, Information Technology Approval Committee, or other entities.

5.2.4 Employees shall submit requests for computer hardware, software or mobile devices by completing a Request & Pre-Acquisition Questionnaire for Microcomputer Equipment and Software, Form 102-1, through their chain of command to the appropriate approving authority.

5.2.4.1 Within five working days of receipt, the CIO shall review and approve the request, approve with modifications, or disapprove the Request & Pre-Acquisition Questionnaire for Microcomputer Equipment and Software form.

5.2.4.2 Requests which do not meet the Departments hardware/software configuration standards shall be returned to the requester, through the chain of command with a memorandum stating recommendations for meeting the required standard.

5.2.4.3 Approved requests are forwarded for processing to the Budget Authority.

5.2.5 For the requisition of telephone lines, data circuits, cell phones, and telecommunication equipment refer to Department Order #104, Communications System.

5.2.6 The requisition of mobile devices (such as tablets or cellular devices), shall be restricted to the Director, Deputy Directors, Assistant Directors, Regional Directors, Wardens, Bureau Administrators, Administrators and CIO. The Director, Deputy Directors, or the Assistant Directors may authorize exceptions.

5.2.7 Request for IT equipment (such as hardware, software, system components, and/or vendor support) shall adhere to the standards set forth in this Department Order. This applies to any item which shall alter the network environment in any way, including the development of test environments and/or remove systems which are connected or have the potential of being connected to the network environment capabilities and allow connection to the Department system.

5.2.7.1 IT hardware standards are available for review at https://azdoc.hpsmartstores.com/.

5.3 Requests for Exceptions to Criteria - When circumstances require the Department to purchase or retain devices or software which does not meet the minimum criteria, the CIO may grant a waiver for the devices or software to continue receiving IT support.

5.3.1 Requests for Exceptions to Criteria justifying a waiver are sent to the CIO, in writing, for review through the chain of command.

5.3.2 A waiver request shall include:

5.3.2.1 A memorandum requesting a waiver review process to be conducted.

5.3.2.2 The business needs for the exceptions and provide technical documentation for the device or application in question.

5.3.2.2.1 IT shall conduct an evaluation of requested exceptions and forward results to the CIO.

5.3.2.2.2 The CIO shall respond to the requester with an explanation of the findings.

6.0 ACCESS TO CORRECTIONS MANAGEMENT INFORMATION SYSTEMS (CMIS) – The following procedure establishes the necessary criteria for designating User authority to access or modify fields and information contained within the CMIS and other Department applications.

6.1 When determining system and information access privileges, including permission or rights to the CMIS or other Department applications, both the approving authority and the IT Applications and Data Manager shall ensure the following: {5-ACI-1F-07}

6.1.1 Special access privileges, including access privileges to sensitive systems such as ACIS and root access on distributed systems, shall be restricted to the greatest extent possible.

6.1.2 Authority for a User to access or modify fields or information within the CMIS or other Department applications shall only be granted in accordance with the Users group or role membership(s).

6.1.3 User authorization shall be based on least privilege required to perform assigned tasks.

6.1.4 Remote access privileges shall comply with section 5.0.

6.1.5 The user roles and permissions should be updated or removed immediately upon job change and termination.

6.1.6 User access review should be performed regularly and audited to minimize risk exposure.

6.2 Responsibility for Actions – Accountability for actions taken regarding the CMIS or other Department applications belongs to the owner of the specific User Identification (ID) under which those actions take place. {5-ACI-1F-07}

6.3 An approving authority wishing an employee to have authority to access or modify fields or information within the CMIS or other Department applications, shall ensure the following forms are completed and submitted to the IT Service Desk for review, approval, and processing prior to being granted access to information: {5-ACI-1F-07}

6.3.1 Non-Disclosure Agreement for Access to Sensitive Information form

6.3.2 ACIS Access Request, Form 102-8.

6.4 The Contract Beds Bureau Monitors shall ensure all contractors who require access to information contained in the CMIS or require the rights to work within the CMIS obtain advance approval from an appropriate approving authority and complete and submit the following forms to the IT Service Desk for review, approval, and processing prior to being granted access to information: {5-ACI-1F-07}

6.4.1 Non-Disclosure Agreement for Access to Sensitive Information form

6.4.2 Internet Use - Reading, Acknowledgment and Receipt, Form 102-4

6.4.3 ACIS Access Request form.

6.5 The IT Service Desk, shall assign approved User Department IDs, verification words, and passwords appropriate to the User authority.

6.5.1 Users who are unable to access systems due to forgotten access numbers and/or verification words shall have their User authority terminated and shall be required to re-apply for User authority through their approving authority.

6.5.2 Users who forget their passwords shall utilize the built in self-service password reset function or contact the IT Service Desk for assistance in retrieving their password.

6.6 User authority regarding the CMIS or other Department applications shall be granted, terminated, modified, or re-evaluated as follows: {5-ACI-1F-07}

6.6.1 Granting, terminating, modifying, or re-evaluating system and information access privileges shall take no more than two business days. Priority processing shall be given based upon the criticality of the situation or the User's need.

6.6.2 User authority shall be: {5-ACI-1F-06}

6.6.2.1 Granted as outlined in 6.5 and 6.6 of this section.

6.6.2.2 Terminated upon User resignation or termination.

6.6.2.3 Terminated or modified for inappropriate behavior as determined by the approving authority.

6.6.2.4 Re-evaluated, modified, or terminated if the User is transferred or reassigned or if the User has a change in duties.

6.6.3 Inactive accounts deemed inactive by the approving authority and/or the IT Service Desk, based upon the nature of the User authority and the frequency of intended versus actual use, shall be terminated.

6.7 External Remote Access Requests – All outside agencies requests for external remote access to the CMIS shall be reviewed and approved by the Offender Services Administrator or designee. The Offender Services Administrator or designee shall determine the validity of the request and the information access privilege. Once approved the request shall be forwarded to the IT Service Desk for processing.

7.0 SYSTEM SECURITY MANAGEMENT

7.1 System Security Program

7.1.1 System Security Plan – The Information Security Officer (ISO) shall distribute, review annually, and update the Department System Security Plan. The System Security Plan shall:

7.1.1.1 Define the authorization boundary for the system including authorized connected devices (e.g., smart phones, authorized virtual office computer equipment, and defined external interfaces).

7.1.1.2 Describe the relationships with or connections to other information systems.

7.1.1.3 Coordinate with other organizational entities.

7.1.1.4 Be reviewed and approved by the CIO for distribution to necessary stakeholders.

7.1.2 System Security Architecture – The system security architecture for the Department information system shall describe the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information.

7.1.3 Security Risk Management – To appropriately manage security risks to the Department's information systems the ISO or designee shall, in accordance with IT Technical Manual: {5-ACI-1F-03}

7.1.3.1 Perform an impact assessment to determine the Department's information system categorization.

7.1.3.2 Categorize the information systems, document the security categorization results (including supporting rationale) in the System Security Plan, and ensure the security categorization decision is reviewed and approved by the CIO. The following system categorization levels shall be applied:

7.1.3.2.1 Standard – Loss of confidentiality, integrity, or availability could be expected to have a limited adverse impact on the Department's operations, organizational assets, or individuals, including citizens.

7.1.3.2.2 Protected – Loss of confidentiality, integrity, or availability could be expected to have serious, severe, or catastrophic adverse impact on organizational, assets, or individuals, including citizens.

7.1.3.3 Conduct a security risk assessment, including the likelihood and magnitude of harm from the unauthorized access, use, disclosure, modification or destruction of the information system and the information it processes, stores or transmits.

7.1.3.3.1 Document security risk assessment results in a report.

7.1.3.3.2 Disseminate security risk assessment results to the CIO and respective Deputy Director, and recommendations to the Director and respective Deputy Director.

7.1.3.4 Scan for vulnerabilities in the Department information system and hosted applications monthly. Vulnerabilities affecting the system/applications are identified and reported.

7.1.4 Security System Program Management – The ISO or designee shall:

7.1.4.1 Ensure plans of action and milestones for the System Security Program and associated information systems are:

7.1.4.1.1 Documented in the organization's planned remedial actions, to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.

7.1.4.1.2 Updated annually based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

7.1.4.1.3 Reviewed for consistency with the organizational risk management strategy and Department-wide priorities for risk response actions for consistency.

7.1.4.2 Maintain an inventory of its information systems, including a classification of all system components (e.g., Standard or Protected).

7.1.4.3 Monitor and report the results of information security measures of performance to the CIO.

7.1.4.4 Maintain the enterprise architecture with consideration for information security and resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Department.

7.1.4.5 Address information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

7.1.4.6 Ensure a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Department associated with the operation and use of Department's information systems; and implement this strategy consistently across the Department.

7.1.4.7 Manage the security state of the Department's information systems and the environments in which those systems operate through security authorization processes.

7.1.4.7.1 Designate individuals to fulfill specific roles and responsibilities within the department risk management process.

7.1.4.7.2 Fully integrate the security authorization processes into a Department-wide risk management program.

7.1.4.8 Define mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Department; and determine information protection needs arising from the defined mission/business processes and revise the process as necessary, until achievable protection needs are obtained.

7.1.4.9 Establish and maintain contact with professional groups and associations specialized in security to:

7.1.4.9.1 Facilitate ongoing security education and training for Department personnel.

7.1.4.9.2 Keep current with recommended security practices, techniques and technologies.

7.1.4.9.3 Share current security-related information including threats, vulnerabilities and incidents.

7.1.5 Security Assessments – The ISO shall ensure the following controls in the assessment and authorization of Department information systems:

7.1.5.1 Assess the security controls in the information system and its environment of operation periodically to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting established security requirements.

7.1.5.2 Independent Assessors – Impartial assessors or assignment teams shall conduct security control assessments. The assessors or assessment team is free from any perceived or real conflict of interest with regard to the development, operation or management of Department information systems under assessment. Security assessment shall be conducted with third parties authorized by the Department that process, store or transmit confidential data.

7.1.6 System Interconnections – The ISO shall:

7.1.6.1 Only authorize connections from the Department information system to other information systems if Interconnection Security Agreements are completed.

7.1.6.2 Document, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated.

7.1.6.3 Review and update Interconnections Security Agreements annually.

7.1.6.3.1 Employing a "deny-all, permit-by-exception" policy for allowing protected Department information systems to connect to external information systems.

7.1.6.3.2 Permitting a third party to process, store, or transmit confidential data, to create, receive, maintain, or transmit confidential information on the Department's behalf only if covered entity obtains satisfactory assurances that the third party will appropriately safeguard the information. IT shall document the satisfactory assurance through a written contract or other arrangement with the third party.

7.1.7 Continuous Monitoring – The ISO shall ensure the Continuous Monitoring Program includes:

7.1.7.1 Monitoring security metrics.

7.1.7.2 Correlation and analysis of security-related information generated by assessments and monitoring.

7.1.7.3 Response actions to address results of the analysis of security-related information.

7.1.7.4 Reporting the security status of IT and the information system to the CIO quarterly.

7.1.8 Penetration Testing – The ISO shall coordinate penetration testing annually on Protected Department information systems from internal and external interfaces. These penetration tests shall include network-layer penetration tests and application-layer penetration tests.

7.1.9 Internal System Connections – IT shall authorize internal connections of other Department information systems or classes of components (e.g., digital printers, laptop computers, mobile devices) to the Department information system, and for each internal connection shall document the interface characteristics, security requirements and the nature of the information communicated.

7.2 Data Classification and Handling – Data created, stored, processed or transmitted on the Department's information systems shall be classified according to the impact to the Department or state citizens resulting from the disclosure, modification, breach or destruction of the data. {5-ACI-1F-01} {5-ACI-1F-06}

7.2.1 Data Classification Categories - All Department data shall be classified as confidential or public. Data that is not specifically identified as confidential is assumed to be public.

7.2.1.1 Confidential Data - Data that shall be protected from unauthorized disclosure based on laws, regulations, and other legal agreements, confidential data includes, but is not limited to:

7.2.1.1.1 System Security Parameters and Vulnerabilities.

7.2.1.1.2 Health information.

7.2.1.1.3 Financial Account Data (on individuals).

7.2.1.1.4 Criminal justice information.

7.2.1.1.5 Critical Infrastructure/Fuel Facility reports.

7.2.1.1.6 Eligible persons.

7.2.1.1.7 Risk assessment and audit records.

7.2.1.1.8 Personal identifying information, such as social security numbers, date of birth, first and last name, etc., except as determined to be public record.

7.2.1.1.9 Licensing, certification, statistics and investigation information of a sensitive nature.

7.2.1.1.10 Other Department-owned and non-Department-owned confidential data.

7.2.1.2 Public Data - Data that may be released to the public and requires no additional levels of protection from unauthorized disclosure.

7.2.2 Handling - All confidential data shall:

7.2.2.1 Only be given to those persons that have proper authorization and a business related "need to know" basis.

7.2.2.2 When hand-carried, be kept with the individual and protected from unauthorized disclosure.

7.2.2.3 Not be left unattended, even temporarily, when outside of controlled areas. All confidential data shall remain either in a controlled environment or in the employee's physical control at all times. Mail, courier, or other mail services are considered controlled areas.

7.2.2.3.1 Unauthorized movement of confidential data from controlled areas shall be prohibited.

7.2.2.4 Be turned over or put out of sight when visitors not authorized to view data are present.

7.2.2.5 Not be discussed outside of controlled areas when visitors not authorized to hear confidential data are present.

7.2.3 Confidential data shall only be processed on approved Department devices, in accordance with this Department Order. Any external transmission of confidential data shall be encrypted.

7.2.4 Media Protection - All confidential data shall be protected using minimum controls as outlined in section 8.0.

7.3 System Security Acquisition

7.3.1 Technology Life Cycle – IT shall ensure information security is included throughout the technology life cycle and integrated into the organizational information security risk management process.

7.3.2 External System Services – The ISO shall require providers of external Department information system services to comply with organizational information security requirements and employ security controls in accordance with applicable federal and state laws, Executive Orders, directives, policies, regulations, standards, and guidance.

7.3.3 Internal System Services – The ISO shall ensure IT development staff performs analyses for threats and vulnerabilities and subsequent testing/evaluation of the Department information system.

7.4 Data Privacy

7.4.1 The Privacy Committee shall determine the legal authority that permits the collection, use, maintenance and sharing of protected information and shall describe the purpose(s) for which protected information is collected, used, maintained and shared. The Privacy Office shall consist of members of the Legal, Human Resources and IT Bureaus.

7.4.1.1 The Department information system enforces approved authorizations for access to protected information in accordance with identity/role-based controls and IT shall employ the concept of least privilege, allowing only authorized accesses to protected information.

7.4.2 Governance and Privacy Program – The Privacy Committee shall:

7.4.2.1 Have a staff member from the Committee act as rotating chair (annually) and agency Officer for Privacy. The Director or a Deputy Director shall approve the Chair.

7.4.2.2 Be accountable for maintaining a Department-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing and disposal of protected information by programs and Department information systems. The Department information systems shall be designed to support privacy.

7.4.2.3 Monitor federal and state privacy laws for changes that affect the privacy program.

7.4.2.4 Develop a strategic privacy plan for implementing applicable privacy controls, policies and procedures.

7.4.2.5 Disseminate operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, Department information systems, or technologies involving protected information.

7.4.2.6 Monitor and audit privacy controls to ensure effective implementation.

7.4.3 Privacy Impact and Risk Assessment – IT shall conduct privacy risk and impact assessments prior to any new collection of protected information or upon significant changes in the architecture, information flow or use of protected information within existing systems.

7.4.4 Privacy Requirements for Contractors and Service Providers – The Privacy Officer shall ensure privacy roles, responsibilities and access requirements are established for contractors and service providers, and include privacy requirements in contracts and other acquisition-related documents.

7.4.5 Accounting of Disclosures – IT, consistent with Department privacy acts and subject to any applicable exceptions or exemptions, shall:

7.4.5.1 Keep an accurate accounting of disclosures of information held in each system of records under its control, including:

7.4.5.1.1 Date, nature, and purpose of each disclosure of a record.

7.4.5.1.2 Name and address of the person or agency to whom/which the disclosure was made.

7.4.5.2 Pursuant to Arizona Revised Statute (A.R.S.) §12-2297, retain the accounting of disclosures for the life of the record or six years after the disclosure is made, whichever is longer or as required by law.

7.4.6 Data Quality – IT shall:

7.4.6.1 Check for, and correct as necessary, any inaccurate or outdated protected information used by its programs or systems annually.

7.4.6.2 Issue guidelines ensuring and maximizing the quality and integrity of disseminated information.

7.4.7 Data Retention and Disposal – IT shall:

7.4.7.1 Retain each collection of protected information for Department defined time period to fulfill the purposes identified in the notice or as required by law.

7.4.7.2 Pursuant to A.R.S. §44-7601 and §41-151.12, dispose of, destroy, erase, and/or anonymize the protected information, regardless of the method of storage, in accordance with an Arizona State Library, Archives and Public Records approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access.

7.4.7.3 Use the media sanitation process outlined in section 8.0, 8.3.1.8 to ensure secure deletion or destruction of protected information (including originals, copies and archived records).

7.4.8 Inventory of Protected Information – The Privacy Officer shall:

7.4.8.1 Maintain and update at least every three years, an inventory that contains a listing of all programs and Department information systems identified as collecting, using, maintaining, or sharing protected information.

7.4.8.2 Provide each update of the protected information use to the CIO and/or ISO at least every three years to support the establishment of information security requirements for all new or modified Department information systems containing protected information.

7.4.9 Internal Use – IT uses protected information internally only as authorized by law or for authorized purpose(s).

7.4.10 Information Sharing with Third Parties - IT shall:

7.4.10.1 Share protected information externally, only as authorized by law or for the authorized purposes identified and described in privacy notice or in a manner compatible with those purposes.

7.4.10.2 Where appropriate, enter into a Department contract, with third parties that specifically describe the protected information covered and the purposes for which the protected information may be used and offers the highest level of protection.

7.5 Vulnerability Management

7.5.1 IT assets must be regularly monitored for vulnerabilities in order to identify where there are information security risks.

7.5.2 Vulnerability Management applies to all information systems and information system components of the Department. Specifically, it includes:

7.5.2.1 Servers, mainframes, and other devices that provide centralized computing capabilities.

7.5.2.2 SAN, NAS, and other devices that provide centralized computing capabilities.

7.5.2.3 Desktops, laptops, and other devices that provide distributed computing capabilities.

7.5.2.4 All other hardware, software, and applications owned and operated by the Department.

7.5.3 IT shall:

7.5.3.1 Perform vulnerability assessment and system patching on a regular basis, and only be performed by designated individuals.

7.5.3.2 List all IT assets, including all hardware and software components, must be accurately in the asset inventory to aid in the management of vulnerabilities.

7.5.3.3 Use vulnerability scanning tools to perform scans of information technology systems to identify information security vulnerabilities. The vulnerability scans shall occur, at a minimum, twice a month.

7.5.3.3.1 The vulnerability scanning tools shall be industry standard, be automated, have definitions updated prior to a scan, utilize credentialed scans, and shall only be accessible by authorized users.

7.5.3.4 Identify vulnerabilities through active monitoring and reviewing of third-party vulnerability sources for any new and unique vulnerability that currently exist.

7.5.3.5 Conduct Security Assessments with a validated third-party in order to identify which vulnerabilities can be exploited by threat actors, in compliance with ADOA-ASET Policy 8120. This assessment will occur annually or when a significant change occurs to the network architecture.

7.5.3.6 Evaluate and assign each vulnerability; an urgency based on the intrinsic qualities of the vulnerability, the criticality of the business systems that it affects, and the sensitivity of the data that can be found on the specific assets.

7.5.3.7 Use one of the following remediation options: patches, configuration changes, or defense-in-depth controls. The exact solution will be identified based on numerous risk factors including the availability of a patch and the risk accepted by utilizing a different method.

7.5.3.8 Accept the risk that comes from leaving the vulnerability open if remediation is not implemented within the time frames outlined in 7.5.3.13.

7.5.3.8.1 The risk acceptance shall include:

7.5.3.8.1.1 The identification of the vulnerability

7.5.3.8.1.2 The justification for risk acceptance

7.5.3.8.1.3 Any compensating controls or remediation plans

7.5.3.8.2 Risk acceptances require the approval of the System Owner, ISO, CIO, and a Deputy Director.

7.5.3.8.3 Risk acceptances will be reassessed on a quarterly basis to validate/update the reasoning for the risk acceptance.

7.5.3.8.4 If a risk acceptance is of a significant and long-term impact the ADOA, Arizona Strategic Enterprise Technology Risk Acceptance Form will be completed and submitted for approval.

7.5.3.8.5 Risk acceptances approved in this manner will only need to be reviewed as outlined on the form.

7.5.3.9 Conduct backups before the implementation of any remediation when possible, in the case that the system needs to be restored.

7.5.3.10 Test all remediation's prior to full implementation since they may have unforeseen side effects. Any exception to testing means that a level of risk is accepted by the Department. This will be documented and approved through the IT Change Control process.

7.5.3.11 Download System and Third-Party application patches from a trusted source.

7.5.3.12 Ensure system patching occurs on a regular basis as outlined below:

7.5.3.12.1 Endpoints

7.5.3.12.1.1 Operating system and third-party product patching shall be assessed and deployed no later than 30 calendar days after the patch has been released.

7.5.3.12.1.2 Critical security updates shall be deployed as soon as possible and within 10 business days of the initial release.

7.5.3.12.2 Server, Appliances, and Other Devices

7.5.3.12.2.1 Operating system and third-party product patching shall be assessed and deployed no later than 30 calendar days after the patch has been released.

7.5.3.12.2.2 Critical security updates shall be deployed as soon as possible and within 10 business days of the initial release.

7.5.3.12.2.3 If a critical security update is released and an existing maintenance window is not within the next 10 business days proper Change Control and staff notifications must be made prior to application of updates.

7.5.3.13 Update all existing configuration and inventory documentation in order to reflect applied remediation by the system owner.

7.5.3.14 Perform audits to ensure that remediation has been applied as required and is functioning as expected.

8.0 SYSTEM SECURITY OPERATIONS

8.1 Configuration Management Plan – The system owners shall ensure the Configuration Management Plan is maintained and documented.

8.2 Emergency Operations Plans

8.2.1 Contingency Plan – The ISO shall ensure the IT Contingency Plan:

8.2.1.1 Identifies and addresses the essential mission and business functions.

8.2.1.2 Provides recovery objectives, and restoration priorities.

8.2.1.3 Identifies contingency roles, responsibilities, assigned individuals with contact information.

8.2.1.4 Addresses maintaining critical mission functionality despite an information system disruption, compromise, or failure.

8.2.1.5 Addresses eventual, full information systems restoration without deterioration of the security safeguards.

8.2.1.6 Is reviewed and approved by the CIO.

8.2.2 Incident Response Plan - The ISO shall ensure the Incident Response Plan: {5-ACI-1F-03}

8.2.2.1 Defines reportable incidents.

8.2.2.2 Defines the resources and management support needed to effectively maintain an incident response capability.

8.2.2.3 Is reviewed and approved by the CIO annually, updated as necessary, distributed to incident response personnel, the Privacy Officer, and communicated to all staff.

8.2.3 Privacy Incident Response Plan – The Department's Chief Counsel, in collaboration with IT, shall pursuant to A.R.S. §44-7501:

8.2.3.1 Investigate potential privacy incidents upon awareness of unencrypted protected information loss.

8.2.3.2 Notify affected parties by telephone, electronic notice or email upon breach determination without unreasonable delay.

8.2.3.2.1 Notification may be delayed if law enforcement determines notification will impede the investigation.

8.2.3.3 For protected information not owned by the Department, notify and cooperate with the owner following the discovery of a breach without unreasonable delay.

8.2.3.4 Provide an organized and effective response to privacy incidents.

8.2.4 Incident Reporting – Pursuant to A.R.S. §41-3507, IT employees shall report suspected cyber security and cyber privacy incidents to the CIO within one hour of knowledge of a suspected incident. The CIO shall report the security incidents information to the ISO, and the privacy incidents information to the Privacy Officer.

8.3 Media Protection

8.3.1 Protected Data

8.3.1.1 Media Marking – IT shall mark information system digital media containing confidential information.

8.3.1.2 Media Storage – Employees shall physically control and securely store digital and non-digital media containing confidential information within controlled areas.

8.3.1.3 Media Transport – IT shall protect and control digital media containing confidential information during transport outside controlled areas.

8.3.1.4 Cryptographic Protection - IT shall employ cryptographic mechanisms to protect information stored on digital media and during transport outside controlled areas.

8.3.1.5 Data Backup – IT shall create a retrievable, exact copy of confidential data, when needed before movement of equipment.

8.3.1.6 IT Restrictions – IT shall employ standards and procedures on the use of removable media in Department information systems.

8.3.1.7 Prohibition of Use Without Known Owner – IT shall prohibit the use of removable media in Department information systems when the media has no identifiable owner.

8.3.1.8 Media Sanitization – IT shall sanitize digital information system media containing confidential information prior to disposal, release of organizational control, or release for reuse.

8.3.1.9 Media Access – IT shall restrict access to protected data.

8.4 Physical Security Protection

8.4.1 Physical Access Authorizations – IT shall:

8.4.1.1 Maintain a list of individuals with authorized access to controlled areas where any protected Department information system resides.

8.4.1.2 Review and approve the access list biannually.

8.4.1.3 Remove individuals from the access list when access is no longer required.

8.4.1.4 Escort and monitor visitor activity within controlled areas.

8.4.2 Protected Data Access Control – IT shall ensure the following physical access controls:

8.4.2.1 Department information system distribution and transmission lines within Department facilities using locked wiring closets; disconnected spare jacks; and/or protection of cabling by conduit or cable trays;

8.4.2.2 Physical safeguards for all workstations that access sensitive information to restrict access to authorized users; and

8.4.2.3 Devices to prevent unauthorized individuals from obtaining output.

8.5 Prohibited Behaviors – The following behaviors may be subject to disciplinary action in accordance with Department Order #601, Administrative Investigations and Employee Discipline: {5-ACI-1F-06}

8.5.1 Employees shall not have administrator rights on Department IT equipment unless there is a legitimate business case, or if their job description calls for administrator rights.

8.5.2 Passwords are not to be shared or requested from employee to employee or supervisor to employee under any circumstances (no exceptions).

8.5.3 Pursuant to A.R.S. §13-2316.1-2, unauthorized access, unauthorized permission escalation, interception, modification or destruction of any computer, Department information system, computer programs or data is prohibited.

8.5.4 Installation or connections of any computing equipment (i.e., desktop/mobile computers, external hard drives, thumb/jump drives, media cards or printers) not provided or authorized by the IT Bureau to Department information systems is prohibited.

8.5.5 Installation or use of any unauthorized software, including but not limited to security testing, monitoring, encryption or "hacking" software on Department computing resources is prohibited.

8.5.6 Software acquisitions and usage shall meet the requirements stated in the applicable vendor software licensing agreement. Apart from the originally approved installation all reproduction installation, and/or use of any state acquired software at work or at another location, such as employee's homes are strictly prohibited.

8.5.7 Use of peer-to-peer file sharing technology used for the unauthorized distribution, display, performance or reproduction of copyrighted work is prohibited. Use of external unauthorized cloud services to transfer confidential data including, but not limited to, personal Google Drive and Drop Box is also prohibited.

8.5.8 Pursuant to A.R.S. §13-2316.3, knowingly introducing a computer contaminant (i.e., virus or malware) into any computer, computer system or Department information system is prohibited.

8.5.9 Pursuant to A.R.S. §13-2316.4, recklessly disrupting or causing the disruption of a computer, computer system or Department information system is prohibited.

8.5.10 Disabling software, modifying configurations, or otherwise circumventing security controls. Tampering with physical security measures (e.g., locks, cameras) is prohibited.

8.5.11 Falsifying identification information, routing information so as to obscure the origins or the identity of the sender, or using/assuming an information system, or application identification other than the employee's own is prohibited.

8.5.12 Pursuant to A.R.S. §38-448, the unauthorized storage, transmission or viewing of any pornography or other offensive, intimidating, hostile or otherwise illegal material is forbidden. Except to the extent required in conjunction with a bona fide Department approved research project or other approved undertaking, an employee shall not knowingly use Department owned or Department leased computer equipment to access, download, print or store any information infrastructure files or services that depict nudity, sexual activity, sexual excitement or ultimate sex acts. (See Department Order #527, Employment Discrimination and Harassment.)

8.5.13 Unauthorized posting of Department draft or final Department documents is prohibited.

8.5.14 Unauthorized Use of Electronic Messaging – The following uses of electronic messaging are prohibited:

8.5.14.1 Sending of unsolicited commercial emails in bulk (identical content to multiple recipients).

8.5.14.2 Creating or forwarding chain letters or pyramid schemes.

8.5.14.3 Sending messages that are unprofessional or un-businesslike in appearance or content.

8.5.14.4 Modification or deletion of email messages originating from another person or computer with the intent to deceive.

8.5.14.5 Falsifying email headers or routing information so as to obscure the origins of the email or the identity of the sender, also known as spoofing.

8.5.14.6 Sending and receiving email using unauthorized or anonymous addresses.

8.5.14.7 Automatically forwarding email sent to a Department account to an external email address without authorization.

8.5.14.8 Unauthorized use of a non-Department email account such as Yahoo or Gmail for Department business.

8.5.14.9 Sending confidential information (e.g., date of birth, social security number, etc.) electronically in a non- secure manner. Confidential information must be sent securely (e.g., encrypted email, SFTP, etc.).

8.5.14.10 Presenting viewpoints or positions not held by the Department as those of the Department or attributing them to the Department.

8.5.15 Personal Use of Department Information Systems – Personal use of Department information systems and information assets while on duty is limited to occasional use during break periods provided that use does not interfere with Department information systems or services. Inappropriate use of Department information systems are prohibited including, but not limited to, the following:

8.5.15.1 Games and entertainment software

8.5.15.2 Trading shares on public or private exchanges

8.5.15.3 Performing or promoting outside business or events

8.5.15.4 Gambling sites

8.5.15.5 Dating sites

8.5.15.6 Using Department email for non-business website registration

8.5.16 Violation of Intellectual Property Laws – Unauthorized receipt, use or distribution of unlicensed software, copyrighted materials or communications of proprietary information or trade secrets.

8.5.17 Unauthorized Access and Release of Confidential Information - Unauthorized access or disclosure of information that has been classified as confidential could cause harm to the Department and/or the citizens of the state. The confidentiality of information is protected by law. The unauthorized access or release/disclosure of any confidential information is prohibited.

8.6 Notifications and Acknowledgements – The following notifications and acknowledgements are to inform those granted access to organizational information and/or Department information systems of steps IT may take to ensure the security of Department information systems. {5-ACI-1F-06}

8.6.1 All state information system assets remain the sole property of the Department. Any data or intellectual property created by the user, including voicemail and electronic messages, remain the property of the Department and should not be removed, copied or shared with any person or entity except as part of the user's normal job responsibilities.

8.6.2 IT Security Office informs all users that it reserves the right to monitor all activities that occur on Department information systems or to access any data residing on its systems or assets at any time without notice. IT Security retains the right to override an individual's passwords and/or codes to facilitate access by the IT Bureau.

8.6.2.1 Users shall have no expectation of privacy for any communication or data created, stored, sent or received on Department information systems and assets.

8.6.2.2 By using Department information systems, users acknowledge that they explicitly consent to the monitoring of such use and the right of IT to conduct monitoring.

8.6.3 The Department may block access to content it deems as inappropriate or filter email.

8.6.4 The Department is not responsible for material viewed or downloaded by users from the Internet or messages delivered to a user's mailbox. Users are cautioned that many Internet pages and emails include offensive, sexually explicit, and inappropriate material. Even though IT intends to filter and block inappropriate content and messages it is not possible to always avoid contact with offensive content on the Internet or in the user's email. If such an action occurs, users are expected to immediately delete the offensive material, leave the offensive site and contact the IT Bureau.

8.6.5 Users shall ensure files, emails, attachments and other records are retained, preserved, and/or disposed of in accordance with the records retention schedule.

8.7 Network Password Requirements

8.7.1 All users shall have a unique password which will be required to be updated every 90 calendar days.

8.7.2 Passwords shall consist of a minimum of 12 characters and shall contain three of the four following elements:

8.7.2.1 Upper case letter

8.7.2.2 Lower case letter

8.7.2.3 Number

8.7.2.4 Special character (e.g., #, @, !, etc.)

8.7.3 Password restrictions are as follows:

8.7.3.1 Use of sequential or repetitive characters (e.g., 12345 or aaaaa)

8.7.3.2 Use of common passwords (e.g., p@ssw0rd, etc.)

8.7.3.3 Use of common dictionary words

8.7.3.4 Use of previous 24 passwords

8.7.4 Users shall lock their PC or log off the network if they are to be away from their computer.

8.7.5 After six consecutive invalid login attempts by a user, the Department information system will automatically lock the account/node for 30 minutes or until released by an administrator when the maximum number of unsuccessful attempts is exceeded.

8.8 Access Agreements - IT shall ensure individuals using:

8.8.1 Computing equipment outside of designated work environments (e.g., virtual offices, working from home or telework centers) acknowledge and accept appropriate access agreements prior to being granted access and review/update agreements annually.

8.8.2 User-based technologies (e.g., smart phones, tablet computers) that access Department information systems as a trusted user acknowledge and accept appropriate access agreements prior to being granted access and review/update agreements annually.

8.9 System Auditing

8.9.1 System owners, in cooperation with IT, shall audit the following events whenever possible and deemed necessary:

8.9.1.1 Password changes

8.9.1.2 Successful and failed logins

8.9.1.3 Successful and failed component access

8.9.1.4 Administrative privilege usage

8.9.1.4.1 Changes to Administrative groups or accounts.

8.9.1.4.2 Escalation of a user account to an administrative account.

8.9.1.4.3 Adding or deleting users from an administrator account.

8.9.1.5 Third-party credential usage

8.9.1.6 Failure or successful access to system objects (i.e., files)

8.9.1.7 Access to audit trails

8.9.1.8 The creation, modification, or deletion of:

8.9.1.8.1 Group accounts.

8.9.1.8.2 User accounts.

8.9.1.8.3 Account privileges.

8.9.2 The audit records shall contain the following information:

8.9.2.1 What type of event occurred

8.9.2.2 When the event occurred

8.9.2.3 Where the event occurred

8.9.2.4 The source of the event (name of data, system component, or resource)

8.9.2.5 The outcome of the event

8.9.2.6 The identity of the individuals or subjects associated with the event

8.9.3 Audit records shall be retained for 90 calendar days when practical/reasonable.

8.9.3.1 In the event that records cannot be retained for an appropriate period a risk acceptance will need to be completed and approved by the System Owner, ISO, CIO, and a Deputy Director.

8.9.4 The auditing system will generate an alert when the audit events fail to process.

8.9.5 System owners are responsible for developing appropriate processes for monitoring and analyzing their audit records.

8.9.5.1 Audit records shall be reviewed periodically for indications of inappropriate or unusual activity.

8.9.5.1.1 All findings shall be reported to the Information Security Office.

8.9.5.1.2 The review process shall employ automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.

8.9.5.1.3 The review process shall analyze and correlate audit records across different repositories to gain situational awareness.

8.9.5.2 The auditing process allows for on-demand audit review, analysis, and reporting.

8.9.5.2.1 The process shall not alter the original audit records.

8.9.5.2.2 The audit records can be processed based on the following fields:

8.9.5.2.2.1 Individual identities

8.9.5.2.2.2 Event types

8.9.5.2.2.3 Event locations

8.9.5.2.2.4 Event times and time frames

8.9.5.2.2.5 Event dates

8.9.5.2.2.6 System resources involved, IP addresses involved

8.9.5.2.2.7 Information object accessed

8.9.6 The auditing process will utilize internal time clocks to generate time stamps for audit records.

8.9.6.1 The time stamps shall be generated into a format that can be mapped to Coordinated Universal Time (UTC).

8.9.6.2 The time stamps shall provide granularity to the unit of time of one second. Additional granularity is allowed.

8.9.6.3 The auditing process shall routinely synchronize time with a centralized system clock.

8.9.6.4 Time synchronization settings are protected so that such settings are restricted to authorized personnel and logging, monitoring, and reviewing changes.

8.9.7 Audit information and tools shall be protected from unauthorized access, modification, or deletion.

8.9.7.1 Access and management of the audit functionality shall be restricted by the System Owner to authorized personnel only.

8.9.7.2 Audit trail files shall be backed up promptly to a centralized log server or media that is difficult to alter.

8.9.7.3 Audit records shall be backed up onto a physically different system or system component than the system or system component being audited.

8.9.7.4 Audit records shall be protected with file integrity monitoring and change detection software to ensure that existing log data cannot be changed without generating alerts. New audit data being added to audit logs do not cause such alerts.

IMPLEMENTATION

The CIO shall maintain the appropriate technical manuals addressing, at a minimum, the following:

- Standardized training guidelines in cooperation with the Chief Learning Officer.
- Processes and procedures used to sanitize computers and other electronic devices.
- Procedures for notifying involved individuals when a security breach in IT compromises personal information.
- Procedures for formal project management of IT projects, programs and systems in accordance with state and industry standards.
- Procedures for System Security Management.
- The annual review of this Department Order.

DEFINITIONS/GLOSSARY

Refer to the Glossary of Terms

FORMS LIST

102-1, Request & Pre-Acquisition Questionnaire for Microcomputer Equipment and Software
102-2, Email Search Request
102-3, Non-Disclosure Agreement for Access to Sensitive Information
102-4, Internet Use - Reading, Acknowledgement and Receipt
102-6, Security Request
102-7, Internet Browsing History Request
102-8, ACIS Access Request

AUTHORITY

A.R.S. §12-2297, Retention of Records
A.R.S. §13-2316, Computer Tampering; Venue; Forfeiture; Classification
A.R.S. §36-342, Disclosure of Information; Prohibition
A.R.S. §36-666, Violation; Classification; Immunity
A.R.S. §38-448, State Employees; Access to Internet Pornography Prohibited; Cause for Dismissal; Definitions
A.R.S. §41-151.12, Records; Records Management; Powers and Duties of Director; Fees; Records Services Fund
A.R.S. §41-1750.01, National Crime Prevention and Privacy Compact
A.R.S. §41-3507, Statewide Information Security and Privacy Office; Duties; Suspension of Budget Unit's Information Infrastructure
A.R.S. §41-4172, Anti-identification Procedures
A.R.S. §42-2001, Definitions
A.R.S. §44-7501, Notification of Breach of Security System; Enforcement; Civil Penalty; Preemption; Exceptions;
Definitions
A.R.S. §44-7601, Discarding and Disposing of Records Containing Personal Identifying Information; Civil Penalty; Enforcement; Definition

A.A.C R2-15-3005, Disposal of Information Technology Assets Directive
Arizona Department of Administration Memorandum, dated 05-18-2010, ADOA SPMO Disposal of Information Technology Assets Directive Revision: 1.1 May -2010 1, Arizona Department of Administration Surplus Property Management Office, Authority: A.A.C. R2-15-303
Arizona Department of Administration/Arizona Strategic Enterprise Technology (ASET)
State Standard Project Investment Justification (PIJ) Policy, P340-S340 Rev-3.0
National Institute of Standards and Technology (NIST)
Health Insurance Portability and Accountability Act (HIPPA)
Internal Revenue Service Publication 1075 (IRS Pub 1075)