CHAPTER: 100

Agency Administration/Management

DEPARTMENT ORDER:

102 – Information Technology

OFFICE OF PRIMARY RESPONSIBILITY:

AS

Arizona Department of Corrections

Department Order Manual

Effective Date:

February 11, 2017

Amendment:

N/A

Supersedes:

DO 102 (2/7/14)

Scheduled Review Date:

TBD

ACCESS

☐ **Contains Restricted Section(s)**

Charles L. Ryan, Director

TABLE OF CONTENTS

PURPOSE

This Department Order establishes standards for the development and integration of efficient, cost-effective information systems to support the Department's 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.

1.2 Human Resources or designee shall notify Information Technology (IT) by email at nteam@azcorrections.gov when an employee retires or terminates employment.

1.3 The Deputy Director, Division Directors and Assistant Director shall:

1.3.1 Identify one or more levels of the approving authority in their area of responsibility to ensure appropriate review and submission of Request for Service (RFS) and New Project Requests (NPR) in accordance with sections 4.0 and 5.0 of this Department Order.

1.3.2 Appoint one or more employees to serve as members of the Subject Matter Expert (SME) Committee.

1.4 The Executive Team shall approve, disapprove, revise, prioritize or take other appropriate action on IT projects related to Department strategy.

1.5 The Department's Chief Information Officer (CIO) shall:

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

1.5.2 Review requests for new equipment and systems for compliance with the Agency Five Year Strategic Plan and Department policy and procedures.

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

1.5.3.1 Designing and installing systems.

1.5.3.2 Maintaining and repairing computers, peripheral and telecommunications equipment.

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

1.5.4 Cooperate with institutions and bureaus when planning system expansions, including:

1.5.4.1 Transfer and control of equipment and software.

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

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

1.5.6 Manage all RFSs and NPRs received by IT in accordance with this Department Order.

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

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

1.5.9 Install and maintain data management systems to collect, store, retrieve and process essential information regarding:

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

1.5.9.2 The Corrections Management Information Systems (CMIS) which are mainframe applications consisting of the Adult Information Management System (AIMS), the Arizona Financial System (AFIS), and other network-based applications residing on any Departmental Local Area Network (LAN) and/or Wide Area Network (WAN) server(s).

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

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

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

1.5.13 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 to the ADOA/Arizona Strategic Enterprise Technology (ASET) Office.

1.6 The SME Committee shall:

1.6.1 Be responsible for reviewing NPRs to identify Department-wide patterns and for taking appropriate action in accordance with section 5.0 of this Department Order.

1.6.2 Meet with the Executive Team on a quarterly basis to make recommendations concerning NPRs with Department-wide strategic and/or resource impact and to provide a briefing of NPRs approved by the SME Committee.

1.7 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.

1.8 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 Arizona Department of Corrections (ADC) staff production data and the Internet.

1.9 Training

1.9.1 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.)

1.9.1.1 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 has taken and completed the "Information Technology and Security Awareness" Computer Based Training course.

1.9.2 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.

1.10 Employees shall ensure possession of personal telephonic communication equipment is in accordance with Department Order #513, Employee Property.

1.11 Agency 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.

1.12 Supervisors shall ensure employees 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 distribute as indicated on the form.

1.12.1 The Contract Beds Bureau Monitors shall:

1.12.1.1 Ensure all contractors who require access to personal and/or confidential information complete and sign a Non-Disclaimer Agreement for Access to Sensitive Information form prior to being given access to information.

1.12.1.2 Forward the original signed forms to the CIO, maintain a copy for their records, and provide a copy for the contractor.

2.0 AUTOMATED OFFICE SYSTEMS - EMAIL AND MESSAGING

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 Agency'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.

2.2.3 Only IT shall install mail messaging client software on employee workstation computers.

2.2.4 The CIO shall evaluate each new version of the mail messaging software and recommend whether or not the Department shall adopt the new version. No upgrades shall be installed without the approval of the CIO.

2.3 Email Access

2.3.1 Authorized employees may be granted an email account based on job function.

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 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 post office.

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 10 Megabyte (MB), or whenever possible for smaller size attachments, shall be sent as a link. Contact Network Services Support at ittechsupport@azcorrections.gov for any assistance.

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 Purging and Archiving

2.6.1 Purging is the process of removing/deleting obsolete information from the email system.

2.6.2 Archiving is the method used to save items indefinitely.

2.7 Department Email

2.7.1 Each mailbox shall have a quota of 2.6 gigabyte (GB). When this quota is reached, the mailbox shall not be able to send or receive email. The system shall automatically generate a warning message prior to the limit being reached to alert the user immediate action is required to reduce the mailbox size. If no action is taken to reduce the mailbox size or an exception is not approved, the user shall not be able to send or receive email. Exceptions to this quota may be approved by the approving authority.

2.7.1.1 Due to the volume of the email messages and associated storage space requirements noted above, the email system shall purge messages automatically according to the following schedule:

2.7.1.1.1 "Trash" container items purged every 14 calendar days. The system shall empty the messages from the mailbox. Users may use self-service recovery in order to retrieve a purged message for an additional 14 days.

2.7.1.1.2 "Sent Items" purged every 90 calendar days. After 90 calendar days, these messages shall be placed in a folder called "Sent Items," directly under the "Deleted Items" folder. They shall be held there for an additional 14 days before being purged.

2.7.1.1.3 Any email message a mailbox owner intends to save indefinitely shall be placed in the designated "Email Retention Folder" (or user defined subfolders below this folder) which resides under "Managed Folders." Messages may also be retained by archiving the message to an archive file on the user's network home directory or "H" drive. Managed Folders and archived folders shall be exempt from automated cleanup.

2.7.1.1.4 Staff shall periodically review email messages in their system folders to prevent the "Email Retention Policy" from deleting important email(s) from their inbox, sent items, etc.

2.7.1.1.5 "Inbox" items regardless of whether or not they have been opened are purged every 90 calendar days. After 90 calendar days, the system shall place these messages in a folder called "Inbox" directly under the "Deleted Items" folder. They shall be held there for an additional 14 days before being purged.

2.7.2 Users may also retain messages by saving the message to an archive file on the network home directory or "H" drive. Messages retained in this way shall not be counted in the 2.6 GB storage quota.

2.7.3 Users may contact Network Services Support at ittechsupport@azcorrections.gov for assistance.

2.7.4 The "Calendar", "Task", and "Notes" in the messaging system are user controlled and are not purged automatically. To avoid storage problems, users shall delete or archive these items regularly. When a permanent record is necessary, the item shall be archived. In all other instances, the item shall be purged.

2.8 Email Search Requests

2.8.1 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:

2.8.1.1 Reason for the request

2.8.1.2 Case number(s), if applicable

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

2.8.1.4 Searchable "key" words

2.8.1.5 Specific dates of inquiry

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

2.8.2.1 Director

2.8.2.2 Deputy Director

2.8.2.3 General Counsel

2.8.2.4 Inspector General

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

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

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

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

2.8.4.2 Enter and record the information outlined in 2.8.4.2.1 through 2.8.4.2.10 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:

2.8.4.2.1 Requestor

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

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

2.8.4.2.4 Case number(s), if applicable

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

2.8.4.2.6 Approving authority

2.8.4.2.7 Date of approval

2.8.4.2.8 Date request received by IT E-discovery staff

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

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

2.9 Upon completion of the requested search, the IT 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.

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

3.0 LAN/WAN HARDWARE AND TELECOMMUNICATIONS INFRASTRUCTURE – All acquisitions of hardware, software, licenses as well as all replacement software for Department networks and all requisitions of telecommunications infrastructure components and equipment including radios, shall meet the criteria, be reviewed and approved as outlined in section 6.0 of this Department Order.

4.0 REQUESTS FOR SERVICE PROCEDURE

4.1 The Request for Service (RFS) process shall be used to address basic operational problems with existing systems, relating to repairing or restoring current functionality. This process shall not include requests for system/screen enhancements, modifications or the development of new applications. The problems are addressed in five IT areas:

4.1.1 Network Services

4.1.2 Applications Systems

4.1.3 Network Infrastructure

4.1.4 Telecommunications

4.1.5 Web Services

4.2 IT provides the following services for the RFS process:

4.2.1 Network Services Support (computer adds, changes, deletes and repairs; email and access to Intranet/Internet).

4.2.2 Applications Systems Support (mainframe, personal computers and web applications).

4.2.3 Network Infrastructure Support (Local Area Network and Wide Area Network).

4.2.4 Telecommunications Support (Cable television (CATV), Cabling Video Conferencing, standard telephone and inmate telephones).

4.2.5 Web Services Support (ADCnet intranet website and internet website (https://corrections.az.gov/) page adds, changes, deletes and repairs).

4.3 Network Services Support

4.3.1 Any basic computer operational difficulties, such as those listed in 4.2.1 above, shall be forwarded to IT using the on-line Department Self-Serve ticket.

4.3.2 IT shall process the requests and notify the user within three business days of either completion or need for additional time due to complexity or other reasons.

4.4 Application Systems Support

4.4.1 Users shall submit requests which meet the RFS criteria as outlined in section 4.0 of this Department Order, using the on-line RFS ticket.

4.4.2 The IT Unit Manager shall review the requests. If the request meets the criteria for a RFS as outlined in this Department Order, the IT Unit Manager shall take one of the following actions:

4.4.2.1 Approve the request and assign the RFS to IT staff.

4.4.2.2 Notify the user within three business days of either completion or need for additional time due to complexity or other reasons.

4.4.2.3 Return the request to the user for clarification.

4.4.2.4 Deny the request. All denials shall provide a reason for the denial to the user.

4.4.2.4.1 If the request meets the criteria for a new project return the request to the user with instructions to submit an NPR in accordance with section 5.0 of this Department Order.

4.5 Network Infrastructure Support

4.5.1 LAN/WAN requests, such as items outlined in 4.2.3 of this section, for maintenance or service cover: hardware, software and/or system component enhancements which affect and/or alter the network environment, including the development of test environments and remote systems which are connected to the local or wide-area networks.

4.5.2 Requests for LAN/WAN Infrastructure Support shall be emailed to the Local IT Specialist identifying the following information:

4.5.2.1 The requestor's demographics, including but not limited to: name, date, division, location, department, telephone number, and email address.

4.5.2.2 A detailed description of the business needs to be addressed.

4.5.3 The Local IT Specialist shall:

4.5.3.1 Respond to the request within 15 minutes up to five business days based on severity level type (critical, urgent, important, monitor, and informational) of the receipt of the request by contacting the requester and initiating the repair process or services, or notifying the requester additional time is required.

4.5.3.2 Log all requests and track the progress of the request to completion.

4.5.3.3 Requests for New Systems or sub-systems shall follow the IT Project procedure for proposing and developing IT projects as outlined in section 5.0 of this Department Order.

4.6 Telecommunications Support

4.6.1 Telecommunications requests cover maintenance of CATV, cabling and infrastructure for telephone and/or data, inmate phones, telephone and video conferencing systems. Any basic telephone operational difficulties shall be forwarded to IT using the on-line ADC Self-Serve ticket, such as those listed in 4.2.4 of this section.

4.6.1.1 Requests for Telecommunications Support shall be emailed to the Local IT Specialist identifying the following information:

4.6.1.1.1 The requester’s demographics, including but not limited to: name, date, division, location, department, telephone number, and email address.

4.6.1.1.2 A detailed description of the business needs to be addressed.

4.6.2 The Local IT Specialist shall:

4.6.2.1 Respond to the request within 15 minutes up to five business days based on severity level type (critical, urgent, important, monitor and informational) of the receipt of the request by contacting the requester and initiating the repair process or services, or notifying the requester additional time is required.

4.6.2.2 Log all requests and track the progress of the request to completion.

4.6.2.3 Requests for New Systems or sub-systems shall follow the IT Project procedure for proposing and developing IT projects as outlined in section 5.0 of this Department Order.

4.7 WEB Services Support – Web Services, as outlined in 4.2.5 of this section include, but are not limited to, Internet (https://corrections.az.gov/), Intranet and any other Department Web application framework.

4.7.1 For any minor update, maintenance, or repair of a web page(s), contact the Webmaster via the Media Relation Office, in person, by telephone or email at webmaster@azcorrections.gov.

4.7.2 For more advance web services not covered above in 4.7.1, requests shall follow IT Project Procedure in 5.0 of this Department Order.

5.0 NEW PROJECT REQUEST PROCEDURE – The following procedure shall be followed for proposing and developing new applications/systems and/or expanded functionality of existing applications/systems for applications systems, network infrastructure, telecommunications (including radios), and web services.

5.1 Staff shall submit all NPRs through their chain of command to the approving authority designated for their area.

5.1.1 The approving authority shall:

5.1.1.1 Ensure requests are completed in accordance with this Department Order.

5.1.1.2 Approve, ask, for clarification, or deny NPRs.

5.1.1.3 Forward approved NPRs to the IT Unit Manager.

5.1.2 The IT Unit Manager shall review all NPRs and take one of the following actions:

5.1.2.1 Forward the request to the SME Committee.

5.1.2.2 Deny the request and return it to the user. All denials shall include reasons for the denial.

5.1.2.3 Return the request to the user with a request for additional clarification.

5.1.2.3.1 Users shall resubmit the revised request as a NPR.

5.1.3 The SME Committee shall:

5.1.3.1 Meet quarterly to review NPRs which have been forwarded to them by the IT Unit Manager.

5.1.3.1.1 The IT Unit Manager shall serve as chair of the SME Committee representing IT subject matter experts.

5.1.3.2 Review each request based on criteria established in the IT Technical Manual to include available resources, and take one of the following actions:

5.1.3.2.1 Approve and assign to IT.

5.1.3.2.2 Combine multiple related requests and assign to IT.

5.1.3.2.3 Return the request to the user for additional clarification. The user may resubmit the request as a new NPR.

5.1.3.2.4 Deny with explanation.

5.1.3.3 Determine if the project relates to the Department's strategic initiatives and goals require significant resources, and/or be a long term project involving multiple divisions. The SME Committee shall present the request, along with a recommendation, to the Executive Team for review and disposition. The recommendation shall include a discussion of the priority of the NPR.

5.1.3.3.1 The SME Committee shall brief the Executive Team quarterly on approved IT projects and present NPRs to the Executive Team for their review and disposition.

5.1.3.3.2 The Executive Team shall approve, disapprove, prioritize, revise and/or take other action.

5.1.4 At the quarterly briefing, the CIO and/or the IT Unit Manager shall provide information concerning IT workload and resource availability to assist the Executive Team in prioritizing and re-prioritizing the Department's IT projects.

5.1.5 The IT Unit Manager shall ensure requesters and approving authorities are notified of the decision of the Executive Team.

5.1.6 Approved NPRs with a financial impact shall be process in accordance with section 6.0 of this Department Order.

5.2 Exceptions and Appeals

5.2.1 Approving authorities may appeal the IT Unit Manager and the SME Committee's denials to the CIO.

5.2.2 Decisions of the Executive Team are final.

5.2.3 The IT Unit Manager or CIO may bring urgent NPRs to the SME Committee and/or the Executive Team between quarterly meetings, as necessary. These shall generally relate to specific Department strategic issues, agency goals, legislative requirements, and/or other critical or time sensitive initiatives.

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

6.1 All requests for acquiring new technology shall comply with Department Order #302, Contracts and Procurement and be reviewed by the ADC technology oversight committee.

6.2 All projects shall comply with the ASET policy.

6.2.1 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 (PO's) sent to the Procurement Officer.

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

6.2.3 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 or Information Technology Approval Committee or other entities.

6.2.4 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.

6.2.4.1 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.

6.2.4.2 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.

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

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

6.2.6 The requisition of mobile devices (such as notepads, I-pads, etc.), shall be restricted to the Director, Deputy Director, Division Directors, Assistant Director, Regional Directors, Wardens, Bureau Administrators, Administrators and CIO. The Director, Deputy Director, Division Directors or the Assistant Director may authorize exceptions.

6.2.7 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.

6.2.7.1 IT hardware and software standards are available for review at http://azdoc.mserver.us/.

6.2.7.2 Any mobile device purchased shall have email.

6.3 Small electronic calculators and simple electronic organizers are not restricted and may be purchased through normal procurement procedures. These devices are usually used independently of other computer devices and are limited in scope. Staff shall consult with their Budget Unit Manager prior to purchase.

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

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

6.4.2 A waiver request shall include:

6.4.2.1 A memorandum requesting a waiver review process is conducted.

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

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

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

7.0 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.

7.1 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:

7.1.1 Special access privileges, including access privileges to sensitive systems such as AIMS and root access on distributed systems, shall be restricted to the greatest extent possible and require identification codes different from those used in normal circumstances.

7.1.2 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).

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

7.1.4 Remote access privileges shall comply with section 6.0 of this Department Order.

7.2 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.

7.3 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 Applications and Data Manager for review, approval, and processing prior to being granted access to information:

7.3.1 Non-Disclosure Agreement for Access to Sensitive Information form

7.3.2 Security Request, Form 102-6

7.3.3 Mainframe Access Request form or Mainframe Access Request (Multiple) form located on the ADOA-ASET website

7.4 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 Applications and Data Manager for review, approval, and processing prior to being granted access to information:

7.4.1 Non-Disclosure Agreement for Access to Sensitive Information form

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

7.4.3 Mainframe Access Request form or Mainframe Access Request (Multiple) form located on the ADOA-ASET website

7.4.4 Security Request form

7.5 The Data Applications and Management Office, under the authority of the IT Applications and Data Manager, shall assign approved User ADC access numbers, verification words, and passwords appropriate to the User authority.

7.5.1 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.

7.5.2 Users who forget their passwords shall contact the CMIS/AIMS coordinator or IT Network Services for assistance in retrieving their password.

7.6 User authority regarding the CMIS or other Department applications shall be granted, terminated, modified, or re-evaluated as follows:

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

7.6.2 User authority shall be:

7.6.2.1 Granted as outlined in 7.5 and 7.6 of this section.

7.6.2.2 Terminated upon User resignation or termination.

7.6.2.3 Terminated or modified for inappropriate behavior as determined by the approving authority and/or IT Applications and Data Manager.

7.6.2.4 Re-evaluated, modified, or terminated if the User is transferred or re-assigned or if the User has a change in duties.

7.6.3 Inactive accounts deemed inactive by the approving authority and the IT Applications and Data Manager, based upon the nature of the User authority and the frequency of intended versus actual use, shall be terminated.

7.7 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 CMIS Coordinator for processing.

8.0 SYSTEM SECURITY MANAGEMENT

8.1 System Security Program

8.1.1 System Security Plan - The Chief Information Security Officer (CISO) shall distribute, review annually, and update the Department System Security Plan. The System Security Plan shall:

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

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

8.1.1.3 Coordinate with other organizational entities.

8.1.1.4 Be reviewed and approved by the CIO.

8.1.2 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.

8.1.3 Security Risk Management – To appropriately manage security risks to the Department's information systems the CISO or designee shall, in accordance with IT Technical Manual:

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

8.1.3.2 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:

8.1.3.2.1 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.

8.1.3.2.2 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.

8.1.3.3 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.

8.1.3.3.1 Document security risk assessment results in a report.

8.1.3.3.2 Disseminate security risk assessment results to the CIO, Division Director for Administrative Services and recommendations to the Director and Deputy Director.

8.1.3.4 Scan for vulnerabilities in the Department information system and hosted applications monthly and when new vulnerabilities potentially affecting the system/applications are identified and reported from internal and external interfaces.

8.1.4 Security System Program Management – The CISO or designee shall:

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

8.1.4.1.1 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.

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

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

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

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

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

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

8.1.4.6 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.

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

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

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

8.1.4.8 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.

8.1.4.9 Ensure the cross-discipline insider threat incident handling team monitors the insider threats are monitored and remediated.

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

8.1.4.10.1 Facilitate ongoing security education and training for Department personnel.

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

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

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

8.1.5.1 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.

8.1.5.2 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.

8.1.6 System Interconnections – The CISO shall:

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

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

8.1.6.3 Review and update Interconnections Security Agreements annually.

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

8.1.6.3.2 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.

8.1.7 Continuous Monitoring – The CISO shall ensure the Continuous Monitoring Program includes:

8.1.7.1 Monitoring security metrics.

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

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

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

8.1.8 Penetration Testing – The CISO shall conduct 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.

8.1.9 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.

8.2 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.

8.2.1 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.

8.2.1.1 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:

8.2.1.1.1 System Security Parameters and Vulnerabilities.

8.2.1.1.2 Health information.

8.2.1.1.3 Financial Account Data (on individuals).

8.2.1.1.4 Criminal justice information.

8.2.1.1.5 Critical Infrastructure/Fuel Facility reports.

8.2.1.1.6 Eligible persons.

8.2.1.1.7 Risk assessment and audit records.

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

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

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

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

8.2.2 Handling - All confidential data shall:

8.2.2.1 Only be given to those persons that have authorized access and a need to know the information in the performance of their duties.

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

8.2.2.3 For IT transfers/receipt containing 500 or more confidential records, be monitored and accounted for to ensure the data is not lost and potentially compromised.

8.2.2.4 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.

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

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

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

8.2.3 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.

8.2.4 Media Protection - All confidential data shall be protected using minimum controls as outlined in section 9.0 of this Department Order.

8.3 System Security Acquisition

8.3.1 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.

8.3.2 External System Services – The CISO 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.

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

8.4 Data Privacy

8.4.1 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.

8.4.1.1 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.

8.4.2 Governance and Privacy Program – The Privacy Committee shall:

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

8.4.2.2 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.

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

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

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

8.4.2.6 Monitor and audit privacy controls to ensure effective implementation.

8.4.3 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.

8.4.4 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.

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

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

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

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

8.4.5.2 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.

8.4.6 Data Quality – IT shall:

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

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

8.4.7 Data Retention and Disposal – IT shall:

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

8.4.7.2 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.

8.4.7.3 Use the media sanitation process outlined in section 9.0 of this Department Order to ensure secure deletion or destruction of protected information (including originals, copies and archived records).

8.4.8 Inventory of Protected Information – The Privacy Officer shall:

8.4.8.1 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.

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

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

8.4.10 Information Sharing with Third Parties - IT shall:

8.4.10.1 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.

8.4.10.2 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.

9.0 SYSTEM SECURITY OPERATIONS

9.1 Configuration Management Plan – The CISO shall ensure the Configuration Management Plan is maintained and documented in accordance with the IT Technical Manual.

9.2 Emergency Operations Plans

9.2.1 Contingency Plan – The CISO shall ensure the IT Contingency Plan:

9.2.1.1 Identifies and addresses the essential mission and business functions.

9.2.1.2 Provides recovery objectives, and restoration priorities.

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

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

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

9.2.1.6 Is reviewed and approved by the CIO.

9.2.2 Incident Response Plan - The CISO shall ensure the Incident Response Plan:

9.2.2.1 Defines reportable incidents.

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

9.2.2.3 Is reviewed and approved by the CIO annually and distributed to incident response personnel, and the Privacy Officer.

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

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

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

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

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

9.2.3.4 Provide an organized and effective response to privacy incidents.

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

9.3 Media Protection

9.3.1 Protected Data

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

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

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

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

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

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

9.3.1.7 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.

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

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

9.4 Physical Security Protection

9.4.1 Physical Access Authorizations – IT shall:

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

9.4.1.2 Issue authorization credentials.

9.4.1.3 Review and approve the access list and authorization credentials annually.

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

9.4.1.5 Escort and monitor visitor activity within controlled areas.

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

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

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

9.4.2.3 Department information system output devices to prevent unauthorized individuals from obtaining output.

9.5 Prohibited Behaviors – The following behaviors may be subject to disciplinary action in accordance with Department Order #601, Administrative Investigations and Employee Discipline:

9.5.1 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.

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

9.5.3 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.

9.5.4 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.

9.5.5 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.

9.5.6 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.

9.5.7 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 such as google drive and drop box is also prohibited.

9.5.8 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.

9.5.9 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.

9.5.10 Pursuant to A.R.S. §13-2316, disabling software, modifying configurations, or otherwise circumventing security controls. Tampering with physical security measures (e.g., locks, cameras) is prohibited.

9.5.11 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.

9.5.12 Pursuant to A.R.S. §38-448, and §13-2316.5, 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.)

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

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

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

9.5.14.2 Creating or forwarding chain letters or pyramid schemes.

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

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

9.5.14.5 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.

9.5.14.6 Sending and receiving email using unauthorized or anonymous addresses.

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

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

9.5.14.9 Sending confidential information (e.g., date of birth, social security number, etc.) over email or other electronic messaging without adequate encryption, including sending this information to a trusted destination.

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

9.5.15 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:

9.5.15.1 Games and entertainment software

9.5.15.2 Trading shares on public or private exchanges

9.5.15.3 Performing or promoting outside business or events

9.5.15.4 Gambling sites

9.5.15.5 Dating sites

9.5.15.6 Using ADC email for non-business website registration

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

9.5.17 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.

9.6 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.

9.6.1 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.

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

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

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

9.6.3 The Department may block access to content it deems as inappropriate or filter email destined for your mailbox.

9.6.4 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.

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

9.7 Network Password Requirements

9.7.1 All users shall have a unique password that changes every 90 days. Passwords shall consist of eight characters and shall contain three of the four following elements:

9.7.1.1 Upper case letter

9.7.1.2 Lower case letter

9.7.1.3 Number

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

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

9.8 Access Agreements - IT shall ensure individuals using:

9.8.1 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.

9.8.2 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.

IMPLEMENTATION

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

- Uniform written standards and the identification of uniform data characteristics and security requirements for the Department.
- Written instructions governing the completion, routing and other uses of forms related to CMIS.
- Standardized training guidelines in cooperation with the Staff Development and Training Bureau Administrator.
- 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.
- Criteria and guidelines for review and disposition of RFSs and NPRs.
- 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

ATTACHMENTS

Attachment A – RFS and New Project Request Process Flowchart

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

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)

ATTACHMENT A

RFS AND NEW PROJECT REQUEST PROCESS FLOWCHART

The intent of this process is to balance the day-to-day tactical needs of the Department with strategic initiatives by establishing review, approval and prioritization processes which maximize human and financial resources dedicated to Information Technology.