

 <p>ARIZONA DEPARTMENT OF CORRECTIONS</p> <p>DEPARTMENT ORDER MANUAL</p>	<p>CHAPTER: 100</p> <p>AGENCY ADMINISTRATION/MANAGEMENT</p>	<p>OPR:</p> <p>AS</p>
	<p>DEPARTMENT ORDER: 102</p> <p><i>INFORMATION TECHNOLOGY</i></p>	<p>SUPERSEDES:</p> <p>DO 102 (01/05/07) DI 302 (03/14/11)</p>
		<p>EFFECTIVE DATE:</p> <p>FEBRUARY 7, 2014</p> <p>REPLACEMENT PAGE REVISION DATE:</p> <p>OCTOBER 3, 2014</p>

TABLE OF CONTENTS

PURPOSE		
APPLICABILITY		
PROCEDURES		PAGE
102.01	GENERAL RESPONSIBILITIES	1
102.02	AUTOMATED OFFICE SYSTEMS - EMAIL AND MESSAGING	3
102.03	LAN/WAN HARDWARE, RADIOS, SOFTWARE, LICENSES AND TELECOMMUNICATIONS INFRASTRUCTURE	7
102.04	REQUESTS FOR SERVICE PROCEDURE	7
102.05	NEW PROJECT REQUEST PROCEDURE	10
102.06	REQUESTS FOR WORKSTATION, LAN/WAN HARDWARE, SOFTWARE AND MOBILE DEVICES.....	12
102.07	INTERNET USE	13
102.08	MOBILE DEVICES SECURITY.....	14
102.09	MEDIA DEVICE SANITIZATION AND DISPOSAL	15
102.10	ACCESS TO SECURITY FOR THE MANAGEMENT INFORMATION SYSTEM	16
	IMPLEMENTATION	17
	DEFINITIONS	18
	CROSS REFERENCE INDEX	20
	AUTHORITY	20
	ATTACHMENTS	

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 Contract Beds facilities. Information systems operated by Contract Beds facilities shall be governed by contract where it is necessary for the private computer system to interface with Department systems.

PROCEDURES

102.01 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 e-mail at nteam@azcorrections.gov when an employee retires or terminates employment.
- 1.3 The Deputy Director, Division Directors, and the 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 (NPRs) in accordance with sections 102.04 and 102.05 of this Department Order.
 - 1.3.2 Appoint one or more employees to serve as members of the Subject Matter Expert (SME) Committee (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) 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, each Division Director and the 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 102.05 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.
 - 1.8.1 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.)
 - 1.8.2 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 Employees shall ensure possession of personal cell phones are in accordance with Department Order #513, Employee Property.
- 1.10 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.
- 1.11 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.
 - 1.11.1 The Contract Beds Bureau Monitors shall:
 - 1.11.1.1 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.
 - 1.11.1.2 Forward the original signed forms to the CIO, maintain a copy for their records, and provide a copy for the contractor.

102.02 AUTOMATED OFFICE SYSTEMS - E-MAIL AND MESSAGING

- 1.1 The use of automated office systems shall be in accordance with ASET E-MAIL Policy P401 dated January 15, 2008. For more current information, access ASET policy located at <https://aset.az.gov/resources/policies-standard-and-procedures>.
 - 1.1.1 Employees shall only use the Department's automated office systems for official business and for approved solicitation requests.

- 1.1.2 A solicitation request via e-mail is allowed only if the request has been submitted and approved by the Director, Deputy Director, Division Directors or the Assistant Director in accordance with Department Order #111, Solicitation.
- 1.1.3 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.
- 1.1.4 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.)
- 1.1.5 E-mails shall contain a proper "Complimentary Close."
 - 1.1.5.1 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.
 - 1.1.5.2 Proper complimentary closing shall include any of the following:
 - 1.1.5.2.1 Sincerely.
 - 1.1.5.2.2 Regards.
 - 1.1.5.2.3 Respectfully.
 - 1.1.5.2.4 No complimentary closing. (Some instances do not call for a complimentary closing.)
 - 1.1.5.3 E-mail signatures shall only contain name, title and contact information. No quotes, sayings or other items are permitted.
- 1.1.6 Employees shall ensure e-mails contain the following information:
 - 1.1.6.1 This e-mail 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.

1.2 Initial Set-Up and Upgrades

- 1.2.1 The Agency's IT shall maintain the e-mail system, software, and maintain standards for the Department.
- 1.2.2 New installations or upgrades to the automated office system shall be coordinated through and approved by the CIO or an appropriate designee.
- 1.2.3 Only IT shall install mail messaging client software on employee workstation computers.
- 1.2.4 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.

- 1.3 E-mail Access
 - 1.3.1 Authorized employees may be granted an e-mail account based on job function.
 - 1.3.2 Temporary, short-term and contract employees shall be assigned an e-mail address upon request from the approving authority.
 - 1.3.3 Automated office system software may be installed on “shared use” or shift computers used for work upon request from the appropriate approving authority.
 - 1.3.4 A Department e-mail client, program or capability shall not be installed on a computer which inmates have access.
- 1.4 Broadcast E-mails – Broadcast e-mails are a general message which is sent to a large number of users or an entire post office.
 - 1.4.1 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.
- 1.5 Approved Broadcast E-Mails - An attachment of greater than 10 Megabyte (MB) or whenever possible for smaller size attachments to a broadcast e-mail shall be sent as a link. Contact Network Services Support at ittechsupport@azcorrections.gov for any assistance.
- 1.6 Delegate Rights
 - 1.6.1 Individuals may give access to their mailbox to co-workers. In addition, staff may share e-mail folders and calendars with co-workers which may need access to the information.
 - 1.6.2 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.
- 1.7 Purging and Archiving
 - 1.7.1 Purging is the process of removing/deleting obsolete information from the e-mail system.
 - 1.7.2 Archiving is the method used to save items indefinitely.
- 1.8 Department E-mail
 - 1.8.1 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 e-mail. 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 e-mail. Exceptions to this quota may be approved by the approving authority.

- 1.8.1.1 Due to the volume of the e-mail messages and associated storage space requirements noted above, the e-mail system shall purge messages automatically according to the following schedule:
 - 1.8.1.1.1 “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.
 - 1.8.1.1.2 “Sent Items” – 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.
 - 1.8.1.1.3 Any e-mail message a mailbox owner intends to save indefinitely shall be placed in the designated “E-mail 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.
 - 1.8.1.1.4 Staff shall periodically review e-mail messages in their system folders to prevent the “E-mail Retention Policy” from deleting important e-mail(s) from their inbox, sent items, etc.
 - 1.8.1.1.5 “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.
- 1.8.2 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.
- 1.8.3 Users may contact Network Services Support at ittechsupport@azcorrections.gov for assistance.
- 1.8.4 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.
- 1.9 Training - Supervisors shall have Department network users complete the annual training requirements of “Information Technology and Security Awareness” Computer Based Training course. (See Department Order #509, [Employee Training and Education.](#))

1.10 Email Search Requests

1.10.1 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:

1.10.1.1 Reason for the request.

1.10.1.2 Case number(s), if applicable.

1.10.1.3 Custodian(s) whose emails are the subject of the search.

1.10.1.4 Searchable “key” words.

1.10.1.5 Specific dates of inquiry.

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

1.10.2.1 Director.

1.10.2.2 Deputy Director.

1.10.2.3 General Counsel.

1.10.2.4 Inspector General.

1.10.3 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.

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

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

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

1.10.4.2 Enter and record the information outlined in 1.10.4.2.1 through 1.10.4.2.10 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:

1.10.4.2.1 Requestor.

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

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

- 1.10.4.2.4 Case number(s), if applicable.
- 1.10.4.2.5 Custodian(s) whose emails are the subject of the search.
- 1.10.4.2.6 Approving Authority.
- 1.10.4.2.7 Date of approval.
- 1.10.4.2.8 Date request received by IT E-discovery staff.
- 1.10.4.2.9 E-discovery delivery date – The date the requested data was delivered to the requestor.
- 1.10.4.2.10 E-discovery delivery receipt – The person the data was delivered to.

1.10.5 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.

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

102.03 LAN/WAN HARDWARE, RADIOS, SOFTWARE, LICENSES, AND TELECOMMUNICATIONS INFRASTRUCTURE

- 1.1 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 102.06 of this Department Order.
- 1.2 Security System - All users shall have a password. A password consists of eight characters and shall contain three of the four following elements:
 - 1.2.1 Upper case letter.
 - 1.2.2 Lower case letter.
 - 1.2.3 Number.
 - 1.2.4 Special character (e.g., #, @, !, etc.).
- 1.3 Employees shall not share passwords with coworkers.
- 1.4 Users shall log off the network if they are to be away from their computer.
- 1.5 Existing microcomputers, hardware, software and telecommunications, equipment may continue to be used as long as they can function and properly integrate with existing/upgraded systems.

- 1.6 Use of Personally Owned Software - To prevent operating conflicts between the network and application software, and to avoid legal issues related to licensing requirements, personally-owned software shall not be loaded on Department-owned electronic devices. This applies to any software or freeware, whether loaded from the Internet or any other source.
- 1.7 Adherence to Software Licensing Requirements - The approving authority and the CIO shall ensure all software acquisitions and usage 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.
- 1.8 Use of personally owned hardware to include desktop/mobile computers, external hard drives, thumb/jump drives, media cards, printers or any other peripheral device is prohibited.

102.04 REQUESTS FOR SERVICE PROCEDURE

- 1.1 The Request for Service (RFS) process shall be used to address basic operational problems with existing systems, relating to repairing or restoring current functionality. The problems are addressed in five IT areas:
 - 1.1.1 Network Services.
 - 1.1.2 Applications Systems.
 - 1.1.3 Network Infrastructure.
 - 1.1.4 Telecommunications.

REST OF PAGE BLANK

1.1.5 Web Services.

1.1.5.1 This process shall not include requests for system/screen enhancements, modifications or the development of new applications.

1.2 IT provides the following services for the RFS process:

1.2.1 Network Services Support (Computer adds, changes, deletes and repairs; E-mail and access to Intranet/Internet).

1.2.2 Applications Systems Support (Mainframe, Personal Computers and Web Applications).

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

1.2.4 Telecommunications Support (Cable television (CATV), Cabling Video Conferencing, Standard Telephone and Inmate Telephones).

1.2.5 Web Services Support (ADCnet intranet website and internet website (<https://corrections.az.gov/>) page's adds, changes, deletes and repairs).

1.3 Network Services Support

1.3.1 Any basic computer operational difficulties, such as those listed in 1.2.1, shall be forwarded to IT using the on-line Department Self-Serve ticket at <http://adccherwell/cherwellselfservice/>.

1.3.2 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.

1.4 Application Systems Support

1.4.1 Users shall submit requests which meet the RFS criteria as established in section 102.04 of this Department Order, using the on-line RFS ticket at <http://10.6.0.58/RFS/default.aspx>.

1.4.2 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:

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

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

1.4.2.3 Return the request to the user for clarification.

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

1.4.2.4.1 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 102.05 of this Department Order.

1.5 Network Infrastructure Support

- 1.5.1 LAN/WAN requests, such as items outlined in 1.2.3 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.
- 1.5.2 Requests for LAN/WAN Infrastructure Support shall be e-mailed to the Local IT Specialist identifying the following information:
 - 1.5.2.1 The Requestor's demographics, including but not limited to: name, date, division, location, department, telephone number, and e-mail address.
 - 1.5.2.2 A detailed description of the business needs to be addressed.
- 1.5.3 The Local IT Specialist shall:
 - 1.5.3.1 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.
 - 1.5.3.2 Log all requests and track the progress of the request to completion.
 - 1.5.3.3 Requests for New Systems or sub-systems shall follow the IT Project procedure for proposing and developing IT projects as outlined in section 102.05 of this Department Order.

1.6 Telecommunications Support

- 1.6.1 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 at <http://adccherwell//wellselfservice/>, such as those listed in 1.2.4 of this section.
 - 1.6.1.1 Requests for Telecommunications Support shall be e-mailed to the Local IT Specialist identifying the following information:
 - 1.6.1.1.1 The requester's demographics, including but not limited to: name, date, division, location, department, telephone number, and e-mail address.
 - 1.6.1.1.2 A detailed description of the business needs to be addressed.
- 1.6.2 The Local IT Specialist shall:

- 1.6.2.1 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.
- 1.6.2.2 Log all requests and track the progress of the request to completion.
- 1.6.2.3 Requests for New Systems or sub-systems shall follow the IT Project procedure for proposing and developing IT projects as outlined in section 102.05 of this Department Order.

1.7 WEB Services Support

- 1.7.1 Web Services, as outlined in 1.2.5 of this section include, but are not limited to, Internet (<https://corrections.az.gov/>), Intranet and any other Department Web application framework.
 - 1.7.1.1 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 e-mail at webmaster@azcorrections.gov.
 - 1.7.1.2 For more advance web services not covered above in 1.7.1.1, requests shall follow IT Project Procedure in 102.05 of this Department Order.

102.05 **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.

- 1.1 Staff shall submit all NPR's through their chain of command to the approving authority designated for their area.
 - 1.1.1 The approving authority shall:
 - 1.1.1.1 Ensure requests are completed in accordance with this Department Order.
 - 1.1.1.2 Approve, ask, for clarification, or deny NPR's.
 - 1.1.1.3 Forward approved NPR's to the IT Unit Manager.
 - 1.1.2 The IT Unit Manager shall review all NPR's and take one of the following actions:
 - 1.1.2.1 Forward the request to the SME Committee.
 - 1.1.2.2 Deny the request and return it to the user. All denials shall include reasons for the denial.
 - 1.1.2.3 Return the request to the user with a request for additional clarification.
 - 1.1.2.3.1 Users shall resubmit the revised request as a NPR.

- 1.1.3 The SME Committee shall:
 - 1.1.3.1 Meet quarterly to review NPR's which have been forwarded to them by the IT Unit Manager.
 - 1.1.3.1.1 The IT Unit Manager shall serve as chair of the SME Committee representing IT subject matter experts.
 - 1.1.3.2 Review each request based on criteria established in the IT Technical Manual to include available resources, and take one of the following actions:
 - 1.1.3.2.1 Approve and assign to IT.
 - 1.1.3.2.2 Combine multiple related requests and assign to IT.
 - 1.1.3.2.3 Return the request to the user for additional clarification. The user may resubmit the request as a new NPR.
 - 1.1.3.2.4 Deny with explanation.
 - 1.1.3.3 If the SME Committee shall determine the project may relate 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.
 - 1.1.3.3.1 The SME Committee shall brief the Executive Team quarterly on approved IT projects and present NPR's to the Executive Team for their review and disposition.
 - 1.1.3.3.2 The Executive Team shall approve, disapprove, prioritize, revise, and/or take other action.
- 1.1.4 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.
- 1.1.5 The IT Unit Manager shall ensure requesters and approving authorities are notified of the decision of the Executive Team.
- 1.1.6 Approved NPR's with a financial impact shall be process in accordance with section 102.06 of this Department Order.

1.2 Exceptions and Appeals

- 1.2.1 Approving authorities may appeal the IT Unit Manager and the SME Committee's denials to the CIO.
- 1.2.2 Decisions of the Executive Team are final.

- 1.2.3 The IT Unit Manager or CIO may bring urgent NPR's 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.

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

- 1.1 All requests for acquiring new technology shall comply with Department Order #302, Contracts and Procurement regarding review by the ADC Technology Oversight Committee.
- 1.2 All projects shall comply with the ASET policy.
 - 1.2.1 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.
 - 1.2.2 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.
 - 1.2.3 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.
 - 1.2.4 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.
 - 1.2.4.1 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.
 - 1.2.4.2 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.
 - 1.2.4.3 Approved requests are forwarded for processing to the Budget Authority.
 - 1.2.5 For the requisition of telephone lines, data circuits, cell phones, and telecommunication equipment refer to Department Order #104, Communications System.

- 1.2.6 The requisition of mobile devices (such as notepads, I-pads, etc.), shall be restricted to the Director, the Deputy Director, Division Directors, the Assistant Director, Regional Directors, Wardens, Bureau Administrators, Administrators, and the CIO. The Director, Deputy Director, Division Directors or the Assistant Director may authorize exceptions.
- 1.2.7 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.
 - 1.2.7.1 IT hardware and software standards are available for review at <http://azdoc.mserver.us/>.
 - 1.2.7.2 Any mobile device purchased shall have e-mail.
- 1.3 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.
- 1.4 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.
 - 1.4.1 Requests for Exceptions to Criteria justifying a waiver are sent to the CIO, in writing, for review through the chain of command.
 - 1.4.2 A waiver request shall include:
 - 1.4.2.1 A memorandum requesting a waiver review process is conducted.
 - 1.4.2.2 The business needs for the exceptions and provide technical documentation for the device or application in question.
 - 1.4.2.2.1 IT shall conduct an evaluation of requested exceptions and forward results to the CIO.
 - 1.4.2.2.2 The CIO shall respond to the requester with an explanation of the findings.

102.07 INTERNET USE

- 1.1 With appropriate supervisory authorization, employees with personal computers at their work site may have access to the Internet.
- 1.2 Prior to an employee accessing a computer, supervisors shall ensure the employee reads, understands, and receives a copy of ADOA/ASET Statewide Policy, Internet Use P501, and ARS 38-448, State employees; access to pornography prohibited; cause for dismissal; definitions, and completes and signs the Internet Use - Reading, Acknowledgement and Receipt, Form 102-4. Supervisors shall forward the form to the Personnel Services Unit for placement in the employee's personnel file.

- 1.3 Downloading Software - Due to the danger of viruses, employees shall not download or install software from the Internet.
 - 1.4.1 IT shall ensure personal computers are protected with appropriate virus detection programs.
 - 1.4.2 The use of photographs as "Wallpaper" is authorized, however, as with any office display employees shall use good judgment and taste in placing these items on their computer.
 - 1.4.3 Streaming audio, i.e., music or video for personal use is prohibited.
 - 1.4.4 Assessing social media sites, such as, but not limited to, FACEBOOK, TWITTER, LINKEDIN, MY SPACE, NING, is strictly prohibited without written permission from the appropriate Division Director or Assistant Director.
- 1.5 Removal of unauthorized software - IT staff, who determines downloaded software is adversely affecting the performance of the Personal Computer, shall remove software. Employees shall not re-install software which has been removed by IT staff. IT shall report any reloading of such software to the employee's supervisor.
- 1.6 Employees shall not access any site which contains rude or offensive language, nudity or depictions of nudity, or any type of sexual content.
 - 1.6.1 Employees who check their personal e-mail accounts from Department equipment shall consider the contents of the e-mail in their personal accounts, especially if the contents of the account contain rude or offensive language, nudity or depictions of nudity, or any type of sexual content.
 - 1.6.2 Examples of personal accounts include Hotmail, Yahoo, Gmail, or any web mail accessed through their Internet provider.
 - 1.6.3 Employees who violate the restrictions outlined in this Department Order may be subject to disciplinary action as outlined in Department Order #601, Administrative Investigations and Employee Discipline.
- 1.7 Employees, who accidentally click onto an Internet link which brings up an inappropriate website, shall immediately provide a written report to their supervisor. This report shall describe the situation, and include the date and time the site was accessed. The supervisor shall send the report to their Warden or Bureau Administrator and the CIO.
- 1.8 In accordance with the requirements and prohibitions of this section, supervisors shall make the final decision as to the appropriate use of the Internet or material obtained from the Internet.

102.08 MOBILE DEVICES SECURITY

- 1.1 Mobile device include laptops, cell phones, mobile devices, notepads and I-pads. Requisitions and assignment of these devices shall be in accordance with Department Order #302, Contracts and Procurement.
- 1.2 All mobile devices shall be in compliance with ASET Encryption Technology Policy P800-S850.
- 1.3 Lost or Stolen Devices

1.3.1 The loss or theft of a mobile device shall be immediately reported to the appropriate supervisor. The supervisor shall contact the local IT Network Services Support Specialist with the user's name, phone number and tag number of the device. IT shall immediately erase and de-activate the device, with the exception of laptops.

1.3.1.1 At this time, there is no method to remotely erase a stolen or lost laptop. The user shall report what data was on the laptop to their supervisor.

1.3.2 For lost or stolen mobile devices, cell phones, laptops, or computers follow the procedures outlined in the ASET Breach of Notification Standard Policy P900-S910.

1.4 Deactivation

1.4.1 A mobile device scheduled for deactivation shall be returned to the local Business Manager, who shall coordinate the deactivation with the local IT Network Services Support Specialist. Such devices may be reset for another user.

1.4.2 A laptop scheduled for deactivation shall be returned to the local IT Network Services Support Specialist who shall coordinate the sanitation of the laptop or preparation for surplus.

102.09 MEDIA DEVICE SANITIZATION AND DISPOSAL

1.1 IT shall ensure all new and non-End of Life/End of Service (EOL/EOS) Department owned computers, servers, printers, network, storage, scanners, copiers, fax machines, multi-functional devices or other clients, network components, operating system or application software or storage media are in compliance with ASET Media Sanitizing/Disposal Policy P800-S880. Monitors and other computer equipment which does not store data shall be disposed of as outlined in Department Order #302, Contracts and Procurement.

1.1.1 If the media storage device cannot be erased, or reinitialized, it shall be incinerated or otherwise destroyed. IT shall note such actions on the appropriate sanitization document; see IT Assets Certification Form R5/10 located at http://www.azdoa.gov/agencies/msd/surplus_property/reference_manual.asp#1.

1.1.2 A copy of the sanitization document shall be attached to the parent device and the original shall be maintained by the local IT Specialist.

1.2 IT shall maintain sanitization documents on all sanitized devices. This document shall include the Department tag number, serial number, manufacturer, model and the name of the employee who performed the sanitization. Central Office IT shall maintain a "Master File" record of all disposal documents at Central Office. See IT Assets Certification Form R5/10 located at http://www.azdoa.gov/agencies/msd/surplus_property/reference_manual.asp#1.

1.3 When an area is ready to dispose of aforementioned equipment, the area shall:

1.3.1 Contact the local IT Network Services who shall sanitize the media storage of the device and complete the appropriate sanitization documentation.

1.3.2 Prepare necessary documentation to transfer the device to State Surplus.

102.10 ACCESS TO SECURITY FOR THE MANAGEMENT INFORMATION SYSTEM

- 1.1 This establishes the necessary criteria for designating User authority to access or modify fields and information contained within the CMIS and other Department applications.
- 1.2 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:
 - 1.2.1 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.
 - 1.2.2 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).
 - 1.2.3 User authorization shall be based on least privilege required to perform assigned tasks.
 - 1.2.4 Remote access privileges shall comply with section 102.06 of this Department Order.
- 1.3 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.
- 1.4 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:
 - 1.4.1 Non-Disclosure Agreement for Access to Sensitive Information, Form 102-3.
 - 1.4.2 Security Request, Form 102-6.
 - 1.4.3 Mainframe Access Request form or Mainframe Access Request (Multiple) form located at <http://aset.azdoa.gov/security/forms>.
- 1.5 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:
 - 1.5.1 Non-Disclosure Agreement for Access to Sensitive Information, Form 102-3.
 - 1.5.2 Internet Use - Reading, Acknowledgment and Receipt, Form 102-4.
 - 1.5.3 Mainframe Access Request form or Mainframe Access Request (Multiple) form located at <http://aset.azdoa.gov/security/forms>.
 - 1.5.4 Security Request, Form 102-6.

- 1.6 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.
 - 1.6.1 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.
 - 1.6.2 Users who forget their passwords shall contact the CMIS/AIMS coordinator or IT Network Services for assistance in retrieving their password.
- 1.7 User authority regarding the CMIS or other Department applications shall be granted, terminated, modified, or re-evaluated as follows:
 - 1.7.1 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.
 - 1.7.2 User authority shall be granted as outlined in 1.5 and 1.6 of this section.
 - 1.7.3 User authority shall be terminated upon User resignation or termination.
 - 1.7.4 User authority shall be terminated or modified for inappropriate behavior as determined by the approving authority and/or IT Applications and Data Manager.
 - 1.7.5 User authority shall be re-evaluated, modified, or terminated if the User is transferred or re-assigned or if the User has a change in duties.
 - 1.7.6 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.
- 1.8 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.

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.
- The annual review of this Department Order.

DEFINITIONS

ADULT INFORMATION MANAGEMENT SYSTEM (AIMS) - A host-based electronic data processing system containing the primary inmate database applications used in inmate management systems.

ARIZONA FINANCIAL INFORMATION SYSTEM (AFIS) – The statewide system utilized for general accounting transactions.

APPROVING AUTHORITY – The Director, Deputy Director, Division Directors, Assistant Director, Regional Operation Directors, Warden, Deputy Warden, Bureau Administrator or their designee, who review, approve, and prioritize RFP's as defined in this Department Order.

ARIZONA STATE ENTERPRISE TECHNOLOGY (ASET) OFFICE - In alignment with the strategic missions of state agencies, ASET develops and executes the statewide information technology strategy as well as provides capabilities services and infrastructure to ensure the continuity of mission critical and essential systems for the state of Arizona.

CABLE TELEVISION (CATV) – A system in which television programs are transmitted to the sets of subscribers by cable rather than by a broadcast signal.

COMPUTER HARDWARE - Computer processing units, modems, printers and other physical components used in electronic data processing operations at the mainframe, mid-range and microcomputer levels.

CORRECTIONS MANAGEMENT INFORMATION SYSTEM (CMIS) - A unified, multiple-component, information technology system designed and implemented to support Department management and operations. CMIS includes, but is not limited to, AIMS and LANs.

EMAIL REQUESTS –

- External requests that follow and require formal processing; Litigation, Administrative Investigations, Equal Employment Opportunity (EEO) Investigations, and Public Records Requests. These requests are normally associated with "Case Numbers" that identify the individual Court, Administrative Investigations Unit, and EEO cases. One exception to this norm is Public Records requests which can be made by anyone but still follow a formal process that requires approval and final review by the legal department prior to disclosing information.
- Internal requests that normally require informal processing; requests made by employees. These requests are not normally associated with or a part of a formal investigation.

HAND-HELD COMPUTERS - Any sophisticated electronic organizer and scheduler which operate using an internal computer operating system (OS) and on-board Random Access Memory (RAM). Such devices may include microphones, expansion slots, memory cards, or Universal Serial Bus (USB) connectors and generally are intended to interface with a desktop computer. Brand name examples include the "Palm Pilot," the Handspring "Prism" and the Sony "Palm OS Handheld." Other terms which describe these items include "Personal Peripheral Device" or PPD, "Personal Digital Assistant" or PDA, and "Personal Information Manager" or PIM.

HUMAN RESOURCES INFORMATION SYSTEM (HRIS) - The automated accounting system used to process personnel, payroll, leave and training transactions.

INFORMATION TECHNOLOGY (IT) – The technology involving the development, maintenance, and use of computer systems, software, and networks for the processing distribution of data.

LOCAL AREA NETWORK (LAN) - A group of microcomputers which can communicate with each other and, if desired, can access remote hosts, or other networks over a Wide Area Network. A network consists of one or more file servers, workstations and peripherals. Network users may share the same data and program files, and send messages directly between individual workstations with files protected by means of an extensive security system.

REST OF PAGE BLANK

THIS PAGE BLANK

MAINTENANCE – All actions which have the object of retaining or restoring or fixing defects of an item in or to a state in which it can perform its required function. The actions include the combination of all technical and corresponding administrative, managerial, and supervision actions. These actions have zero scope associated with the system product.

MICROCOMPUTER - A computer built around a microprocessor; a personal computer (PC) with a monitor, keyboard and central processing unit (CPU).

MOBILE DEVICE (Also known as a handheld device, handheld computer or simple handheld) - A small handheld computing device, typically having a display screen with touch input and/or a miniature keyboard and weighing less than two pounds. Mobile device include laptops, cell or smart phones, mobile devices, notepads and I-pads.

NEW PROJECT REQUEST (NPR) – A request submitted by a user to IT for proposing and developing new application/systems and/or expanded functionality of existing applications/systems for applications systems, networks infrastructure, telecommunications (including radios), and web services.

PERIPHERAL - A modem, printer, tape-backup system, mouse or other hardware which is attached to the CPU, generally via cables, and which is usually driven by software.

PERSONAL COMPUTER (PC) – A microcomputer designed for individual use, as by a person in an office or at home, work, or school, for such application as word processing, data management, or financial analysis.

PROJECT MANAGER (PM) – Is the application of knowledge, skills and techniques to execute projects effectively and efficiently. It is a strategic competency for organization, enabling them to tie project results to business goals, thus, better compete in their market.

RETURN ON INVESTMENT (ROI) – A performance measure used to evaluate the efficiency of an investment or to compare the efficiency of a number of different investments. To calculate ROI, the benefit (return) of an investment is divided by the cost of the investment; the result is expressed as a percentage or a ratio.

REQUEST FOR SERVICE (RFS) – A request submitted by a user to IT to address basic operational problems with existing systems, related to repairing or restoring current functionality. The problems are addressed in five IT areas: Network Services, Applications Systems, Network Infrastructure, Telecommunications, and Web Services. (This process shall not include requests for system/screen enhancements or modifications or the development of new applications. See New Project Request (NPR).

SENSITIVE/PERSONAL/CONFIDENTIAL INFORMATION – Per ASET policy, includes any information which may be used to identify an individual, including, but not limited to name, social security number, credit card, charge or debit card number, retirement account number, savings, checking or securities entitlement account number, driver license number or non-operating identification license number, physical description, race, ethnic origin, sexual orientation, income, blood type, DNA code, fingerprints, marital status, religion, home address, home telephone number, education, financial matters, and medical or employment history readily identifiable to a specific individual.

SOFTWARE - An operating system, application program, routine or symbolic language consisting of written or printed instructions which control basic computer hardware functions and tasks. Some examples include; word processing programs, databases, graphics programs, and spreadsheets. This term encompasses any computer language necessary for operation of the system in question, to include; operating systems, utilities, and application software. Included as well is any contractual programming acquired from sources outside the Department and the IT staff.

SUBJECT MATTER EXPERT (SME) COMMITTEE – The SME Committee is composed of representatives of each Division, appointed by members of the Executive Team. As a cross-functional group, the SME Committee reviews individual NPR requests to determine commonalities, trends, and patterns in issues and requests and as a group makes recommendations for disposition as described in the Department Order.

VOICE OVER INTERNET PROTOCOL (VOIP) – A communications protocol which allow for telephonic communication via the internet.

WIDE AREA NETWORK (WAN) - A networking system which covers a large geographic area and includes any computing device which may be permanently or temporarily integrated into a LAN.

WORKSTATION - A microcomputer used by an individual to do his or her work. In a LAN, the term often distinguishes an individual user's PC from a PC used as a shared resource, such as a file server.

{Original Signature on File}

Charles L. Ryan
Director

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

CROSS REFERENCE INDEX

Department Order #103, Correspondence / Records Control
Department Order #104, Communication System
Department Order #111, Solicitation
Department Order #302, Contract / Procurement System
Department Order #509, Employee Training and Education
Department Order #513, Employee Property
Department Order #601, Administrative Investigations and Employee Discipline

AUTHORITY

A.R.S. 38-448, State employees; access to internet pornography prohibited; cause for dismissal; 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.R.S. 41-4172, Anti-identification procedures
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
ASET E-mail Use Policy, P-401
ASET Internet Use, P501

ASET Social Networking Policy, P505
ASET IT Security Policy, P800, Rev 3.0
ASET Encryption Technology Policy, P8800-S850, Rev 3.0
ASET Media Sanitizing/Disposal, P800-S880, Rev 2.0
ASET Information Security Incident Management Policy, P900
ASET Breach of Nonfiction Standard, P900-S910

**ATTACHMENT A
DEPARTMENT ORDER 102**

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.

