 <p>ARIZONA DEPARTMENT OF CORRECTIONS</p> <p>DEPARTMENT ORDER MANUAL</p>	<p>CHAPTER: 100</p> <p>AGENCY ADMINISTRATION/MANAGEMENT</p>	<p>OPR: AS</p>
	<p>DEPARTMENT ORDER: 102</p> <p><i>INFORMATION TECHNOLOGY</i></p>	<p>SUPERSEDES: See Attachment D</p>
		<p>EFFECTIVE DATE: JANUARY 5, 2007</p> <p>REPLACEMENT PAGE REVISION DATE: MARCH 28, 2011</p>

TABLE OF CONTENTS

PURPOSE

APPLICABILITY

PROCEDURES

PAGE

102.01	GENERAL RESPONSIBILITIES.....	1
102.02	AUTOMATED OFFICE SYSTEMS - GROUPWISE	2
102.03	HARDWARE, SOFTWARE, & LICENSES, AND INFRASTRUCTURE	5
102.04	REQUESTS FOR SERVICE	5
102.05	INFORMATION TECHNOLOGY PROJECT PROCEDURE.....	7
102.06	REQUEST FOR WORK STATION AND LAN/WAN HARDWARE AND SOFTWARE.....	10
102.07	INTERNET USE.....	12
102.08	REQUEST FOR WEB SERVICES.....	14
102.09	SECURITY IN THE USE OF PORTABLE/MOBILE ELECTRONIC DEVICES	15
102.10	COMPUTER SANITIZATION.....	16
102.11	ACCESS TO SECURITY FOR THE MANAGEMENT INFORMATION SYSTEM.....	17
	IMPLEMENTATION.....	17a
	DEFINITIONS	17b
	AUTHORITY.....	19
	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 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 prisons. Information systems operated by private prisons 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 and other electronic devices from unauthorized access.
- 1.2 Supervisors and Contract Monitors shall notify Information Technology (IT) by e-mail when an employee retires or terminates employment.
- 1.3 The Department's Chief Information Officer (CIO) shall:
 - 1.3.1 Semi-annually, review and revise Department standards for hardware and software as outlined in Information Technology Standards, Attachment A, for computer systems and networks.
 - 1.3.2 Review requests for new equipment and systems for compliance with the Department's automation plan and Department standards.
 - 1.3.3 Coordinate activities related to computer and telecommunications hardware and software systems such as:
 - 1.3.3.1 Designing and installing systems.
 - 1.3.3.2 Maintaining and repairing computers, peripheral and telecommunications equipment.
 - 1.3.3.3 Ensuring the security of hardware, software, networks and data.
 - 1.3.4 Cooperate with institutions and Bureaus when planning system expansions, including:
 - 1.3.4.1 Transfer and control of equipment and software.
 - 1.3.4.2 Changes in the function of computer and telecommunications hardware and software systems.
 - 1.3.5 Provide analysis input and recommendations to staff regarding their automation requirements.

- 1.3.6 Manage all service requests sent to IT by:
 - 1.3.6.1 Ensuring that all requests received by IT are date-stamped upon receipt.
 - 1.3.6.2 Reviewing all requests within ten work days of receipt for approval, denial or return for clarification. In the event that a review cannot be completed within this time frame due to the complexity of a request, the requestor shall be notified of the expected completion date.
- 1.3.7 Approve or deny requests for exceptions to current standards depending on the specific application and need.
- 1.3.8 Review statewide software applications and requirements, and provide recommendations to the Executive Staff and the Director.
- 1.3.9 Install and maintain data management systems to collect, store, retrieve and process essential information regarding:
 - 1.3.9.1 The network infrastructure linking all Department locations to the Department of Administration (DOA) data center, and other external agencies.
 - 1.3.9.2 The Corrections Management Information Systems (CMIS) mainframe applications consisting of the Adult Information Management System (AIMS), the Uniform Statewide Accounting System (USAS), and other network-based applications residing on any Departmental Local Area Network (LAN) and/or Wide Area Network (WAN) server(s).
- 1.3.10 Provide information about automated technology plans and system capabilities to the Deputy Director and each Division Director.
- 1.3.11 Serve as the Department's representative in programs and projects involving information management issues, including the development of appropriate written instructions.
- 1.3.12 Develop, administer and monitor compliance with the provisions of the Department's Agency Information Technology Plan submitted annually to Arizona's Government Information Technology Agency (GITA.)
- 1.4 Wardens, Deputy Wardens, Administrators, and Bureau Administrators shall ensure that inmates do not have access to CMIS, LAN, WAN, Internet, or any other type of network system or to any computer not specifically authorized.
- 1.5 No one while supervising an inmate shall have in their possession a personal cell phone or computer, unless prior written approval is received by the appropriate Division Director.
- 1.6 All personal cell phones are considered contraband within the secure perimeter of an institution.

102.02 AUTOMATED OFFICE SYSTEMS - GROUPWISE

- 1.1 Use of automated office systems
 - 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 email is allowed only if the request has been submitted and approved in accordance with Department Order #111, Solicitation.
 - 1.1.3 All documents created in the automated office systems are considered public records.

- 1.1.4 The professional standards that apply to Department memorandums, in terms of subject and vocabulary, shall be applied to automated office system communications.
- 1.1.5 E-mail signatures shall only contain name, title and contact information. No quotes, sayings or other items are permitted.
- 1.2 Initial Set-Up and Upgrades - GroupWise office automation software is the standard for the Department.
 - 1.2.1 New installations or upgrades to GroupWise shall be coordinated through and approved by IT or designee.
 - 1.2.2 Only IT staff shall install GroupWise client software on employee workstation computers.
 - 1.2.3 The CIO shall evaluate each new version of the GroupWise software and recommend whether or not the Department should adopt the new version. No upgrades shall be installed without the approval of the CIO.
- 1.3 Email Access - All employees on a Department network shall be assigned an email address.
 - 1.3.1 Temporary, short-term and contract employees shall be assigned an email address office upon request from the Director, the Deputy Director, a Division Director, a Warden, Deputy Warden, Administrator or Bureau Administrator (approving authority).
 - 1.3.2 GroupWise, Microsoft Word, and Word Perfect Office shall be installed on "shared use" computers upon request from the appropriate approving authority.
 - 1.3.3 GroupWise, Microsoft Word, and Word Perfect Office shall not be installed on a computer to which inmates have access.
- 1.4 Broadcast Emails - Broadcast emails are a general message that is sent to a large number of users or an entire post office.
 - 1.4.1 Employees shall use Broadcast - email with discretion.
 - 1.4.2 Supervisors may send broadcast messages to persons in their subordinates.
 - 1.4.3 Users wishing to send a broadcast message outside their downward chain of command shall receive 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.
 - 1.4.4 Broadcast message restrictions do not apply to groups working on a common project and communicating with one another.
- 1.5 System Security - All users shall have a password.
 - 1.5.1 Employees shall not share passwords with coworkers.
 - 1.5.2 Users shall log off the network if they are to be away from their computer for an extended period of time.

1.6 Proxy Rights

1.6.1 GroupWise users may grant "proxy access rights" to other users, which allows the proxy to access one or more of the following grantor's documents:

1.6.1.1 Mail.

1.6.1.2 Calendar.

1.6.1.3 Tasks.

1.6.1.4 Notes.

1.6.2 Proxy access rights may include reading and writing to documents or may be limited to read only. Typically, proxy access rights are limited to "read only." However, "write permission," to any one of the documents listed in 1.6.1 may also be given. Discretion should be used in assigning "write permission" since the action of the proxy, in such cases, cannot be distinguished from that of the granting user.

1.7 Purging and Archiving

1.7.1 Purging is the process of removing/deleting obsolete information from the computer system.

1.7.2 Archiving is the method used to save items indefinitely.

1.7.3 GroupWise E-mail - Due to the volume of email messages and the associated storage space requirements, GroupWise email messages shall be purged automatically according to the following schedule:

1.7.3.1 "Trash" container items every seven calendar days.

1.7.3.2 "Out Box" items every 30 calendar days.

1.7.3.3 "In Box" items, regardless if they have been opened, every 30 calendar days.

1.7.4 Word Perfect email - Due to the volume of E-mail messages, the associated storage space requirements and the lack of an automatic purge feature, Word Perfect email users shall either purge or archive their E-mail messages every 30 calendar days.

1.7.5 Any email messages that a user wants to save indefinitely must be archived (saved) to their "C" drive as a file.

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

1.8 Internet Access from GroupWise - GroupWise includes the capability to send and receive messages via the Internet if Internet access is provided. (Note: GroupWise does not provide access to the Internet itself.)

1.8.1 Internet use shall be limited to employees with approval from the Director, Deputy Director or appropriate Division Director.

1.8.2 Internet use from GroupWise for approved users shall be limited to official business.

1.9 Training - Supervisors shall encourage new GroupWise users to attend formal training. IT shall maintain a current listing of training providers.

1.10 Problem Resolution

1.10.1 Users who experience a GroupWise-related problem shall contact the IT Help Desk for assistance.

1.10.2 IT staff shall contact the caller within one workday of receipt of the call to initiate the problem resolution.

102.03 LAN/WAN HARDWARE, SOFTWARE, & LICENSES, AND TELECOMMUNICATIONS INFRASTRUCTURE - All acquisitions of hardware, software and accompanying licenses as well as all replacement equipment and software for Department networks shall meet the criteria outlined in Attachment A and be approved as specified in section 102.05. All acquisitions of telecommunications infrastructure components and equipment shall be reviewed and approved as specified in section 102.05.

1.1 Telecommunications infrastructure includes all data, voice and video circuits, cable TV, network infrastructure, IP-based telephony, and video conferencing equipment. All requests for new infrastructure or to connect to or expand existing infrastructure shall be submitted in writing detailing the specific needs, suggested options, and benefits.

1.2 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.

1.3 Use of Personally Owned Software - To prevent operating conflicts between network and application software, and to avoid legal issues related to licensing requirements, personally owned software shall not be loaded on a Department-owned computer. This prohibition applies to any software or freeware whether loaded from permanent media or from the Internet or any other source.

1.4 Adherence to Software Licensing Requirements - The Deputy Director, Division Directors, Wardens, Deputy Wardens and Bureau Administrators shall ensure that all software acquisition 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 other locations, such as employee's homes, is strictly prohibited.

1.5 Use of personally owned hardware to include desktop/portable computers, external hard drives, media cards, printers or any other peripheral device is prohibited.

102.04 REQUESTS FOR SERVICE

1.1 This section addresses Requests For Service (RFS) for the following types of support provided by IT:

1.1.1 Technical Support Contacts.

1.1.2 Application Systems Support (Mainframe and PC).

1.1.3 Networks (Local Area Network/Wide Area Network).

1.1.4 Telecommunications (CATV, Network Infrastructure, IP-based Telephony, Video Conferencing).

1.1.5 Standard Telephone System Requests, see Department Order #104, Communications System.

1.2 Technical Support Contacts

1.2.1 The initial contact for technical support shall be referred to as Level 1 Support. The points of contact by location are:

1.2.1.1 For Central Office users: the Central Office Help Desk

1.2.1.2 For institutions, the Information Services Coordinator for CMIS problems, the local IT Network Specialist for PC application problems and the local Telecommunications Specialist for CATV, cabling, telephony and video conferencing problems.

1.2.1.3 For Community Corrections users: the Community Services Information Specialist.

1.2.2 Level 1 Support provides the first line of problem assistance for their respective user groups and manages the specific problem resolution through the various support and priority levels. Level 1 support addresses the most common issues and escalates problem incidents to Level 2 Support that either are beyond the Level 1 support capability or exceed the established deadline for closure. The Level 1 Support Specialist shall track and keep the customer informed throughout the resolution process whether or not a problem is escalated.

1.2.3 Level 2 Support addresses Mainframe, Network, PC Application and Telecommunications problem incidents that are of a more technical or complex nature than Level 1 support can resolve, or that extend beyond the Level 1 time deadline. Level 2 shall escalate unresolved problems to Level 3 support.

1.2.4 Level 3 Support involves issues that cross one or more IT disciplines or are beyond the capability of internal support staff to resolve or that have been drawn out over an extended period of time.

1.3 Application Systems Support (Mainframe and PC) - Within each bureau, section, or institution, approving authorities desiring changes to existing application systems shall:

1.3.1 Complete a Request for Service (RFS), Form 102-2, to request maintenance on a current application system to correct a defect or to request enhancements in the form of additions, changes, or deletions to an existing system. The RFS is submitted to the IT Applications Manager. IT shall time stamp and log the RFS. Upon request, IT shall provide assistance with completing the RFS.

1.3.1.1 In reviewing an RFS for system maintenance the IT Applications Manager shall determine within 15 work days whether the requested change is functional within the scope of an existing system. If not, the request shall either be:

1.3.1.1.1 Returned to the requestor for clarification and conceptual development.

1.3.1.1.2 Denied and returned to the requestor with an explanation of the denial.

1.3.1.2 For any RFS that is approved for development or for any requests that require system enhancements, the IT Application Manager shall advise the requestor of the estimated completion date based upon resource availability, time required for the work, and the priority.

1.3.2 Requests for New Systems B Requests for new mainframe systems or new PC-based systems shall follow the Information Technology Project Procedure for proposing and developing new IT projects. Refer to Section 102.04.

1.3.3 Tracking Requests B IT shall time stamp the RFS and track the progress of the request to completion. IT shall notify the requestor of the disposition on all requests.

1.4 Network Computer Systems and Telecommunications - LAN/WAN Requests for Maintenance or Service comprise any requests (hardware, software or system component enhancements) that affect and/or alter the network environment, including the development of test environments and remote systems that are connected to the local or wide-area networks. Telecommunications Requests cover maintenance or modifications to inmate CATV, cabling and infrastructure for telephone and/or data, telephone and videoconferencing systems.

1.4.1 Requests for Repair are submitted to the Level 1 support specialist in memorandum format identifying the following information:

1.4.1.1 The Requestor's name, date, location, telephone number and e-mail address.

1.4.1.2 A detailed description of the service required or of the problem to be resolved.

1.4.2 The Level 1 support specialist shall:

1.4.2.1 Respond to the request within 2 hours of the receipt of the request by contacting the requestor and initiating the repair process or service, or notifying the requestor that the issue has been escalated to Level 2 support. (Level 2 escalation requires review by the appropriate IT Application, Network or Telecommunications Manager.)

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

1.4.3 Requests for New Systems or sub-systems shall follow the Information Technology Project processes for proposing and developing IT projects as outlined in section 102.04.

102.05 INFORMATION TECHNOLOGY PROJECT PROCEDURE - The following IT project procedure shall be followed for proposing and developing new systems or infrastructure.

1.1 Proposals describing the desired system or infrastructure shall be developed in conjunction with IT staff prior to submission to the appropriate Division Director for review and authorization, and shall include:

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

1.1.2 The proposed benefits to be derived from the new system or infrastructure.

- 1.1.3 Scope of the project and impacts on or involvement required from other Department work units.
- 1.1.4 Suggested solution(s) that will achieve the business objectives.
- 1.1.5 Alternative solutions.
- 1.2 When the appropriate Division Director has approved the proposal, IT staff shall complete a Request for Service (RFS) and submit the request to the CIO for in-depth technical review, development, and recommendations.
- 1.3 The CIO shall review all requests in regard to the following:
 - 1.3.1 Hardware costs for all computer and telecommunications equipment necessary to accomplish the project scope.
 - 1.3.2 Software costs for all operating systems, utility and application software purchased or developed, databases, and all programming required from sources within, and outside of, the Department.
 - 1.3.3 Connectivity costs for all telecommunications circuits, infrastructure, network equipment and software within the scope of the project.
 - 1.3.4 Costs for data conversion, employee training, and system implementation as well as for ongoing support.
 - 1.3.5 Project feasibility in terms of compatibility with existing systems, infrastructure and equipment, and the needed enhancements in the existing environment to meet minimum compatibility requirements with the proposed system.
 - 1.3.6 Project cost analysis including the calculated Return on Investment (ROI) and lifetime operation costs of the system.
- 1.4 The results of the review shall be returned to the Approving Authority of the originating work area in the form of an initial project scope document detailing the findings.
 - 1.4.1 Projects under \$25,000 require the approval of the Division Director and/or the Approving Authority.
 - 1.4.2 For projects with a cost of \$25,000 and over the requesting Division Director shall, in conjunction with the Executive Committee; consisting of the Director, the Deputy Director and the Division Directors, assess costs/benefits, availability of funding and other resources, and project timing in order to allocate funding and/or to define requirements for alternative funding. The Director has sole approval authority. General approval may be awarded with suspension of start dates to coincide with availability of resources.
- 1.5 For projects requiring a Project and Investment Justification (PIJ), IT shall coordinate development of the PIJ document for approval by the Director and submission to the Government Information Technology Agency (GITA) for their review and approval. For projects requiring additional approval from the Information Technology Authorization Committee (ITAC), IT will develop needed presentation materials to solicit ITAC approval.
- 1.6 Once approved by GITA/ITAC, the appropriate Division Director developing the project shall appoint staff to assist IT until the project is implemented.

- 1.7 IT shall work in conjunction with appointed staff, outside vendors, and consultants to complete the project and shall submit monthly progress reports to the Executive Committee through the final implementation of the project. IT shall also submit any periodic reports related to the project required by GITA or ITAC or other entities.
- 1.8 Project Management
 - 1.8.1 Project reports shall include but are not limited to status of project tasks and milestones, schedules, staffing, accomplishments, costs, and any related variances.
 - 1.8.2 Outside consultants shall not be contracted to manage projects or be represented as project managers without specific approval of the Executive Committee.
- 1.9 Project Completion
 - 1.9.1 Upon completion of a project but prior to production implementation, IT shall send a notification through Memo Router or via email, as applicable, with specifics of the changes to be implemented.
 - 1.9.1.1 This notification shall be addressed to management, the Information Service Coordinator, Information Technology Specialists and System Users, as applicable.
 - 1.9.1.2 When notified that a project is being placed into production, the Information Coordinator and/or the Information Specialist shall notify supervisors in the affected local user groups of the changes to the system.
- 1.10 Hand-Held Computers
 - 1.10.1 The assignment of Hand-Held computers, such as " Palm Pilots," shall be restricted to the Director, the Deputy Director, Division Directors, Regional Operations Directors, Regional Health Administrators, Wardens and Facility Health Administrators. The Director may authorize exceptions.
 - 1.10.2 Authorized staff may purchase their device through existing procurement and approval processes for computer hardware. Any device purchased shall have e-mail capability.
 - 1.10.3 Additional purchases may include hardware or software intended to allow the device to easily connect to the Department's network systems and allow the user to access schedules, e-mail or other functions.
 - 1.10.3.1 Connectivity functions may be included with the device or may be purchased separately.
 - 1.10.3.2 Purchases may include docking devices and cradles. An example of connecting technology is referred to as "hotsync".
 - 1.10.4 Small inexpensive 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 very limited in scope. Staff shall consult with the Budget Unit Manager prior to purchase.

102.06 REQUEST FOR WORK STATION AND LAN/WAN HARDWARE AND SOFTWARE

- 1.1 Employees shall submit requests for computer hardware or software 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. Requests for telecommunications support shall be submitted as outlined in Department Order #104, Communications System.
 - 1.1.1 The approving authority shall forward approved requests to the CIO with a completed and approved Request For Purchase, Form 302-2.
 - 1.1.2 Within five work days of receipt, the CIO shall review and approve, approve with modifications, or disapprove the Request & Pre-Acquisition Questionnaire for Microcomputer Equipment and Software.
 - 1.1.2.1 Requests that do not meet established standards shall be returned to the requestor, through the chain of command, with a memorandum stating recommendations for meeting the existing criteria.
 - 1.1.2.2 Approved requests are forwarded for processing to the budget authority shown on the Request for Purchase.
- 1.2 Requests for network equipment or support (hardware, software, system components, and/or vendor support) shall adhere to the standards set forth in Attachment A. This applies to any item that will alter the network environment in any way including the development of test environments and/or remote systems that are connected, or have the potential of being connected, to the network environment.
- 1.3 Desktop and network equipment and/or software requests are divided into four specific categories:
 - 1.3.1 Maintenance/Repair/Refurbishment Items - Those requests to return equipment and related items to their original working condition. The on-site Level 1 support specialist shall review the request for compatibility and reasonability. Upon verification of the request by the Level 1 support specialist, the local purchasing procedures are to be followed.
 - 1.3.1.1 The local approving authority shall review the request, determine the cost effectiveness of maintenance, repair or refurbishment and either approve or disapprove the request.
 - 1.3.1.2 These items are then processed for procurement locally and once received are installed by the local support specialist. These items do not require the use of the Request & Pre-Acquisition Questionnaire for Microcomputer Equipment and Software, unless specifically requested by the appropriate Division Director.
 - 1.3.2 Upgrade Items - These requests expand or increase the original capability of the equipment and related items. The local Level 1 support specialist shall review the request for system compatibility and forward it to the appropriate Level 2 IT Support Manager for a network impact and standards compliance review. Once this review has been accomplished, the Level 2 IT Support Manager shall submit the request to the appropriate approving authority for approval or disapproval.
 - 1.3.2.1 The approving authority shall review the request and determine the cost effectiveness of upgrading the requested items.

- 1.3.2.2 These items are then processed for procurement locally and once received are installed by the local support specialist. These items do not require the use of the Request & Pre-Acquisition Questionnaire for Microcomputer Equipment and Software unless specifically requested by the Deputy Director or appropriate Division Director.
- 1.3.2.3 Disapproved requests are returned to sender with an explanation as to why the request has been disapproved.
- 1.3.3 Replacement Items - These requests replace original equipment with ones having greater capacity. The appropriate Level 1 support specialist shall review requests for end user products (e.g., desktop workstations, laptops, printers, scanners, client-side operating systems and application software.)
 - 1.3.3.1 The Level 1 support specialist shall forward the request in memorandum format, to the appropriate Level 2 IT Support Manager for certification that the requested items meet the standards set forth in Attachment A or a determination that the request does not meet the standards.
 - 1.3.3.1.1 Requests that are certified as meeting the standards shall be forwarded to the appropriate approving authority for approval using a Request & Pre-Acquisition Questionnaire for Microcomputer Equipment and Software. Approved requests are forwarded to the CIO who processes them as specified in 1.1.1 and 1.1.2 of this section.
 - 1.3.3.1.2 Denied requests shall be returned to the original requester with an explanation as to why the request has been denied.
- 1.3.4 New Network Hardware Items - These requests expand or replace current network equipment (e.g. servers, switches, routers, related cabling and software). Requests are sent to the IT Network Manager at Central Office for processing.
 - 1.3.4.1 The Network Manager shall certify that the requested items meet the standards set forth in Attachment A or determine that the request does not meet the standards.
 - 1.3.4.2 Certified requests shall be sent to the requesting area's approving authority for approval using a Request & Pre-Acquisition Questionnaire for Microcomputer Equipment and Software. Approved requests are forwarded to the CIO who processes them as specified above.
- 1.4 Requests for Exceptions to Criteria - When circumstances require the Department to purchase or retain devices or software that do 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 why a waiver is needed are sent to the CIO, in writing, for review. The CIO has final authority regarding the granting of waivers.

- 1.4.2 In order to be considered for a waiver, requestors shall:
 - 1.4.2.1 Prepare a memorandum requesting that a waiver review process be conducted.
 - 1.4.2.2 Ensure that the "Request for Exception to Criteria" states the business needs for the exemption, and provide technical documentation for the device or application in question.
 - 1.4.2.2.1 IT staff shall conduct an evaluation of requested exceptions and forward results to the CIO.
 - 1.4.2.2.2 The CIO shall respond to the requestor with a final disposition and 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. Employees shall engage in work related activities during their assigned duty hours. Personal use of the Internet shall be limited to breaks, lunch periods or, with prior supervisory authorization, during off-duty hours before or after work.
- 1.2 Prior to an employee accessing a computer, supervisors shall ensure that the employee reads and receives a copy of ARS 38-448, State employees; access to internet 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 employee's personnel file. Business related Internet use includes, but is not limited to:
 - 1.2.1 Conducting general research projects.
 - 1.2.2 Accessing the Department's Internet page or the ADCNet.
 - 1.2.3 Obtaining information for grants available to the Department.
 - 1.2.4 Project analysis or research.
 - 1.2.5 Accessing statutes or government rules.
 - 1.2.6 Preparing reports.
 - 1.2.7 Preparation for training.
 - 1.2.8 Ordering products through a business web site in accordance with procurement procedures.
 - 1.2.9 Downloading material or information, including software, when appropriate. Employees shall conform to applicable copyright and licensing regulations.
 - 1.2.10 Communication using e-mail with other business-related entities.
 - 1.2.11 Other business related activity as approved by the employee's supervisor.

- 1.3 Electronic Mail through the Internet shall be used as a method of communication with the public, other professionals or telecommuting.
 - 1.3.1 Electronic mailing shall be in accordance with Department Order #201, Information Release.
 - 1.3.2 All correspondence is a reflection on the Department and remains the property of the Department. The State of Arizona may monitor and log Internet usage by any user with out notice.
 - 1.3.3 Employees shall keep personal email content in good taste and conform to usual standards of written communication.
- 1.4 Downloading Software - Due to the danger of viruses, employees shall not download or install software from the Internet.
 - 1.4.1 Supervisors shall ensure that personal computers are protected with appropriate virus detection programs.
 - 1.4.2 Virus free, shareware, freeware or other software may be used when approved by the appropriate supervisor. Copyright laws shall be observed at all times.
 - 1.4.3 The use of photographs as "Wallpaper" is authorized, however as with any office display employees should use good judgment and taste in placing these items on their computers.
 - 1.4.4 Streaming Audio or Video for personal use is prohibited.
- 1.5 Removal of unauthorized software - IT staff who determine that downloaded software is adversely affecting the performance of the PC, shall remove that software. Employees shall not re-install software that has been removed by IT staff. IT shall report any reloading of such software to the employee's supervisor.
- 1.6 IT shall monitor all Internet traffic and use tracking software, and may use other State agencies/contractors for the purpose of monitoring Internet traffic.
 - 1.6.1 The Department owns all equipment and the access rights; therefore, privacy while using the Internet is not possible.
 - 1.6.2 All records, including e-mail site visit markers are retained automatically.
- 1.7 Any information involving inmates shall be cleared by the appropriate supervisor and conform to the applicable statutes, rules and written instructions. Specific information involving inmates released to the Internet should be fictionalized, except when a matter of public record.
- 1.8 Employees shall not access any site that contains rude or offensive language, nudity or depictions of nudity, or any type of sexual content.
 - 1.8.1 Employees who check their personal e-mail accounts from Department equipment should consider the contents of any e-mail in their personal accounts, especially, if the contents of the account may contain rude or offensive language, nudity or depictions of nudity, or any type of sexual content.

1.8.2 Examples of personal accounts include Hotmail, Yahoo, or any web mail provided by their Internet Services Provider.

1.8.3 Employees who violate the restrictions outlined in the Department Order may be subject to disciplinary action as outlined in Department Order #601, Administrative Investigations and Employee Discipline.

1.9 Employees, who accidentally click on to an Internet link that 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 in which the site was accessed.

1.10 Supervisors shall make the final decision as to appropriate use of the Internet or material obtained from the Internet. Employees shall contact IT for any question involving browsers, search engines or other technical aspects of the Internet.

102.08 REQUEST FOR WEB SERVICES - Web Services includes, but is not limited to, Internet, Intranet, Extranet and any other Department Web application framework.

1.1 Employees (Content Owners) may submit ideas for Web publication by completing and submitting the Web Request For Review Form located on the ADCNet.

1.2 IT Services Content Developers in conjunction with Content Owners shall develop a Web format that conforms to the Web Service template.

1.3 The Content Owner shall indicate approval of the Web format by signing the Web Request For Review Form and forwarding it to the Web Manager for review. The Web Manager may:

1.3.1 Forward the web review form to the Web Support Manager for processing and publication. The Web Support Manager shall e-mail an Action Notification to the Content Owner once the content is published.

1.3.2 Send an Action Notification to the Content Owner that indicates technical issues or the need for content filtering. The notification shall describe the difficulties or technical issues that are preventing the publication and provide viable options.

1.3.3 Initiate a Deferred Action and forward the request to the Content Owner and the Content Owner's Bureau Administrator for review by subject matter experts. This Deferred Action:

1.3.3.1 If approved by the subject matter expert, shall be forwarded to the Web Support Manager for processing and publication.

1.3.3.2 If rejected by the subject matter expert, shall be returned to the Content Owner with an explanation as to why the content of the request was rejected. The Content Owner may resubmit the request once corrections have been made to the request.

1.4 The Web Support Manager shall maintain an archive of Web Contents based upon publication schedules.

1.5 Content Developers shall maintain a copy of Web Contents through the design active timeframes.

1.6 For more information regarding the development and operations of Department websites see Technical Manual 102-IT-Web Services-TM.

- 102.09 SECURITY IN THE USE OF PORTABLE/MOBILE ELECTRONIC DEVICES** - This includes Laptops, Cell Phones and Personal Digital Assistants (PDAs). Requisition and assignments of these devices shall be in accordance with the applicable Department Orders.
- 1.1 Supervisors shall ensure that 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 granted access to that information, and distribute as indicated on the form.
- 1.1.1 Contract Monitors shall ensure that all contractors who require access to personal or confidential information complete and sign a Non-Disclosure Agreement for Access to Sensitive Information form.
- 1.1.2 The Contract Monitor shall forward the original signed form to the Chief Information Officer, maintain a copy for their records and provide a copy to the contractor.
- 1.2 Employees and contractors shall take reasonable steps to protect sensitive material that is stored on portable electronic devices.
- 1.2.1 Employees or contractors who are authorized the use of a state PDA shall:
- 1.2.1.1 Delete emails that are not essential to keep on the PDA or other handheld device.
- 1.2.1.2 Set and enable password protections.
- 1.2.2 Employees or contractors authorized to use state issue cell phones shall:
- 1.2.2.1 Take reasonable steps to protect sensitive material that is stored on cell phones.
- 1.2.2.2 Delete emails or text messages that are not essential to keep on their phones.
- 1.2.2.3 Set and enable password protection.
- 1.2.3 Employees or contractors who are authorized the use of a state Laptop shall:
- 1.2.3.1 Not store unencrypted sensitive and/or personal information on the laptop.
- 1.2.3.2 Not store employee addresses, social security numbers and dates of birth, unencrypted or encrypted.
- 1.2.3.3 Not store written passwords in the laptop case.
- 1.2.3.4 Encrypt sensitive and personal information that must be stored on the laptop. Such information shall only be stored with the approval of an immediate supervisor and only when rights to the data have been granted through Network Administration.
- 1.2.3.5 Not leave the laptop unattended in a non-secure location.
- 1.2.3.6 Not leave the device visible in the car unattended. Devices may be secured in a locked vehicle out of sight.

1.2.3.7 Not check devices with luggage when traveling; staff shall keep devices with them at all times.

1.3 Lost or Stolen Portable Electronic Devices

1.3.1 The loss or theft of a PDA shall be immediately reported to the appropriate supervisor. The supervisor shall contact the IT Enterprise System (ITES) Administrator with the user's name, phone number and tag number of the device. The ITES Administrator shall immediately erase and de-activate the device.

1.3.2 Cell Phone - The loss or theft of the cell phone shall be immediately reported to the appropriate supervisor. The supervisor shall immediately contact the cell phone provider and cancel the service on the device.

1.3.3 Laptop - The loss or theft of a laptop shall be immediately reported to the appropriate supervisor.

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

1.4 Deactivation

1.4.1 A PDA scheduled for deactivation shall be returned to the Business Manager, who shall coordinate the deactivation with the ITES administrator. Such devices may be reset for another user.

1.4.2 A Cell Phone scheduled for deactivation shall be returned to the Business Manager, who shall coordinate the deactivation with the Cell Phone provider.

1.4.3 A laptop scheduled for deactivation shall be returned to the supervisor, who shall coordinate the cleaning of the laptop or preparation for surplus.

102.10 COMPUTER SANITIZATION

1.1 Information Technology shall ensure hard drives are erased, or in the case of Macintosh computers, reinitialized prior to being released to surplus. Monitors and other computer equipment that does not store data shall be disposed of as outlined in Department Order #302, Contracts and Procurement.

1.2 IT shall sanitize computer hard drives to protect against reasonable attempts to recover any data that may have been stored on the hard drive.

1.2.1 If the hard drive cannot be erased, or reinitialized, it will be incinerated or otherwise destroyed. IT shall note such actions on the appropriate sanitization documents. (See Sanitization Document, Attachment B, and the Sanitization Logs, Attachment C.)

1.2.2 A copy of the sanitization document will be attached to the PC and the original will be maintained by the local IT Specialist.

1.3 IT shall maintain sanitization documents on all sanitized computers. This document shall include the ADC 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.

- 1.4 When an area is ready to dispose of a PC, that area shall:
 - 1.4.1 Contact the local IT Specialist who shall sanitize the hard drive of the computer and complete the appropriate sanitization documentation.
 - 1.4.2 Prepare necessary documentation to transfer the PC to State Surplus.

102.11 ACCESS TO SECURITY FOR THE CORRECTIONS MANAGEMENT INFORMATION SYSTEM (CMIS) AND OTHER DEPARTMENT APPLICATIONS

- 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 Information Technology 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 UserID 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 that the following forms are completed and submitted to the Information Technology Applications and Data Manager for review, approval, and processing prior to being granted access to that information:
 - 1.4.1 Non-Disclosure Agreement for Access to Sensitive Information, Form 102-3
 - 1.4.2 Account Request Form, Attachment E
 - 1.4.3 Security Request, Form 102-6
- 1.5 Contract Monitors shall ensure that 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 Information Technology Applications and Data Manager for review, approval, and processing prior to being granted access to that 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 Account Request, Attachment Form E
- 1.5.4 Security Request, Form 102-6
- 1.6 The Data Applications and Management Office, under the authority of the Information Technology 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 will have their User authority terminated and will 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 technical Support 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 will 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 Information Technology 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 Information Technology 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 Information Technology CMIS Coordinator for processing.

IMPLEMENTATION

The CIO shall maintain 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/Training Administrator.
- Processes and procedures used to sanitize computers and other electronic devices.
- **SECTION DELETED**

- Procedures for notifying involved individuals when a security breach in IT compromises personal information.
- The semi-annual review of this Department Order to incorporate recommended technology changes and advancements.

DEFINITIONS

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

APPROVING AUTHORITY - A Deputy Director, Assistant Director, Warden, Deputy Warden, or Bureau Administrator who is responsible for administering the work activities in the unit or institution that requests project development, changes or maintenance to an existing automated system from IT.

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.

HAND-HELD COMPUTER - Any sophisticated electronic organizer and scheduler that operates 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 that 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.

REST OF PAGE BLANK

LOCAL AREA NETWORK (LAN) - A group of microcomputers that can communicate with each other and, if desired, 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.

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

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

SENSITIVE/PERSONAL/CONFIDENTIAL INFORMATION - Includes any information that may be used to identify an individual, including, but not limited to his or her 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, martial 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 that 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 Information Technology staff.

UNIFORM STATEWIDE ACCOUNTING SYSTEM (USAS) - The automated accounting system used by the Department for general accounting transactions.

WIDE AREA NETWORK (WAN) - A networking system that covers a large geographic area and includes any computing device that 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 - ADC Microcomputer Evaluation Standards

Attachment B - Computer Sanitation Document

Attachment C - Computer Disposal Log

Attachment D - Supersedes

Attachment E - Account Request Form/Data Sharing Non-Disclosure/
Employee Verification Word Form

FORMS

102-1, Request & Pre-Acquisition Questionnaire for Microcomputer Equipment and Software

102-2, Request for Service

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. 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

INFORMATION TECHNOLOGY STANDARDS

Purpose - In conjunction with Departmental Order #102, Information Technology, Attachment A provides the necessary criteria for making acquisition and disposition decisions regarding information system hardware or software and their associated licensing. It also defines the levels of Department Information Technology Architecture and the standards against which "Requests for Exceptions to Criteria" can be created.

IT Architecture Levels

User B Information technology under local (user) control, generally considered stand-alone or peer-to-peer systems and their associated applications and services.

Distributive B Information technology having impact on multiple systems and users, generally considered Local Area Networks (LAN) and shared applications and services.

Enterprise B Information technology having impact on multiple distributed systems and users, generally considered a collection of LAN networks or a Wide Area Network (WAN) with accompanying shared applications and services.

Hardware Criteria

IT Desktop Hardware

Devices at the User level must be IBM compatible personal computers. Notebook or desktop styles "form factors" are equally suitable at this level but must meet different criteria as presented in Tables 1.1 B 1.2.

IT Stationary Devices (Workstation PC)

Workstation: a PC configured to allow access to the network for file, print, and application services and which supports multimedia features.

Portable Devices (Notebook PC)

Notebook: a PC assigned for portable use configured to allow access to the network for file, print, and application services.

Selection Criteria

Table 1.1 DESKTOP PC FEATURES MATRIX

CRITERIA CATEGORY	SUB-CATEGORY	WORKSTATION
Enclosure	Case Type	Mini-Tower
	Options	Convertible
	Drive Bays	3 External 2 Internal
Intel Processor	Model	Pentium IV
	Speed	2.4 GHZ (2000 MHZ)
	Onboard Cache	512 KB
Intel Compatible Mother Board	Chipset	Intel 845
	Bus Speed	533 MHZ front side
	Memory (RAM)	512 MB expandable to 2 GB
	Memory Type	ECC DDR 266MHZ
	Expansion Capabilities	5 PCI 1 AGP
	Hard Drive Controller	Ultra ATA/100
	Audio	Integrated
	Network Interface	Integrated Intel 10/100
Storage	Diskette	3.5@ 1.44MB
	Optical	DVD-ROM AND CD-RW
	Hard Drive	40 GB Minimum 7200 RPM OR
Video	AGP	32 MB Minimum
System Restoration	Recovery CD	Required

Quick Reference

Type	Model	Vendor
Workstation	Compaq Evo D510 Convertible Mini Tower	GITA Approved

Note: Quick Reference Models meet or exceed all hardware requirements, and fulfill Desktop Software and Licensing criteria detailed in the corresponding matrices below.

TABLE 1.2 NOTEBOOK PC FEATURES MATRIX

Criteria Category	Sub-Category	Executive Workstation
Enclosure	Clam Shell	2 spindle
	Bays	
Intel Processor	Model	Intel P IV
	Speed	2.2 GHZ (2200 MHZ)
	Cache	2512 KB
Memory	Minimum	512 MB
Storage	Hard Drive	60 GB Minimum
	Diskette	3.5@ 1.44MB
	Optical	CD-RW DVD-ROM Combo Drive
Communications	Network Interface	Mini-PCI V.90 modem 10/100 TX NIC Combo
Audio		Compaq Premier Sound
Visual	Graphics	64 MB
	Display	15" TFT SXGA +
Battery		9 cell Li-Ion
Pointing Device	Type	Touchpad + Pointer

Quick Reference		
Type	Model	Vendor
Notebook	Compaq Evo N800c	GITA Approved

Note: Quick Reference Models meet or exceed all hardware requirements, and fulfill Desktop Software and Licensing criteria detailed in the corresponding matrices below

Server Hardware

Server Hardware Definition - Devices at the Distributive and Enterprise Levels must be fully compatible Intel Architecture and be of the 19-inch Rack mount style "form factor". When specifying a server, the criteria must meet *scale* before *function*. The necessary criteria for acquisition or disposition are presented in Tables 2.1. Acquisitions outside the criteria will only be supported when a waiver has been granted as outlined in Department Order #102.

Server Criteria for Scale:

Branch Office Server: a server performing functions for a single small office or a facility with limited user demand.

Complex Server: a server performing functions for a single high use location or a medium to large facility.

Enterprise Server: a server performing functions for multiple locations, facilities or the entire Departmental WAN.

Typical Server Functions:	Application Server	Network Access Server
	Database Server	Print Server
	FAX Server	Proxy Server
	File Server	Remote Access Server
	Intranet Server	Web Server
	Mail Server	

Servers are designed individually - No quick reference is available

Network Hardware

Network Hardware Definition - Devices providing packet delivery and connectivity within the interior cable plant of a facility's network considered to be on the *Site* or *Branch Office* scale or the *Distributed Level* as defined by the Department's IT Architecture.

Routers

Routers Definition - Devices providing Layer 3 network packet routing between autonomous networks. There are three levels identified within standard architecture. The first two levels are scaled for Branch office and Complex locations, and the necessary criteria for acquisition or disposition are presented in Tables 3.1. Acquisitions outside the criteria will only be supported when a waiver has been granted as outlined in Department Order #102. The devices for exterior connection on the *Enterprise Level* are considered outside the scope of this document's acquisition criteria and must be handled on an individual basis.

Table 3.1 Network Router Features Matrix

Criteria Category	Sub-Category	Branch Office Level	Complex Level	Enterprise Level
Form Factor	Rack Mount	19 Inch	19 Inch	
Regulatory Compliance	FCC	Class B	Class B	
Processor	Type	Motorola MPC860 RISC	IDT R4700 RISC	
RAM Memory	Minimum	64 MB	64 MB	
	Expandable	128 MB	128 MB	
Flash Memory	Minimum	16 MB	16 MB	
	Expandable	32 MB	32 MB	
Interfaces	Network	10/100 Ethernet	10/100 Ethernet	
	WAN slots	2	4	
Operating System Platform	Encryption Software	3DES IPsec	3DES IPsec	
	CISCO compatible	IOS 12.0 or Higher	IOS 12.0 or Higher	
	Firewall	Fully PIX compatible	Fully PIX compatible	

Quick Reference

	Model	Vendor
Branch Office Level	CISCO 2650	GITA Approved
Complex Level	CISCO 3700	GITA Approved

Network Switches

Network Switches Definition - Devices providing packet delivery and connectivity within the interior cable plant of a facility's network. The necessary criteria for acquisition or disposition are presented in Tables 4.1. Acquisitions outside the criteria will only be supported when a waiver has been granted as outlined in Department Order #102.

The Switch Standards are divided into three levels as follows:

Network Switch Segment- Provides Layer 2 packet switching for local segments within a Branch Office or LAN network.

Network Switch Backbone- Provides Layer 2 packet switching between segments or local Network Switch Segments between LAN Networks.

Network Switch Enterprise- Provides Layer 3 packet switching between WAN Networks. This level of networking device is outside the scope of this document.

Table 4.1 Network Switch Features Matrix

Criteria Category	Sub Category	Segment	Backbone	Enterprise
Network Interface	10BaseT/ 100BaseTX Support	12, 24, 48 auto sensing 10Base T/100BaseTX ports	12, 24, 48 auto sensing 10Base T/100BaseTX ports	
Ethernet Interface	Gigabit Ethernet Support		2 built-in, GBIC-based Gigabit Ethernet ports	
	Class of Service Prioritization	IEEE 802.1p combined with two priority queues on 10/100	IEEE 802.1p combined with two priority queues on 10/100	
Security	Virtual LANs on All Ports	Up to 250 port-based VLANs & support for standards-based IEEE 802.1Q	Up to 250 port-based VLANs & support for standards-based IEEE 802.1Q	
Performance Features	Switching Fabric	10.8-Gbps switching fabric & up to a 8.0-Mpps forward rate. 4 MB shared-memory architecture.	10.8-Gbps switching fabric & up to a 8.0-Mpps forward rate. 4 MB shared-memory architecture.	
	Mode	Full-duplex operations on switched 10/100 ports		
	Performance	CGMP Fast Leave	CGMP Fast Leave	
	Management	Cisco Group Management Protocol (CGMP)	Cisco Group Management Protocol (CGMP)	
	Bandwidth	Bandwidth aggregation through Fast EtherChannel technology or Gigabit EtherChannel	Bandwidth aggregation through Fast EtherChannel technology or Gigabit EtherChannel	
	Storm Control	Per-port broadcast storm control.		

Quick Reference

	Model	Vendor
Backbone Level	CISCO Catalyst 3508G XL	GITA Approved
Segmenting Level	CISCO Catalyst 2950 /24port CISCO Catalyst 2950 /48port	GITA Approved

Client Software

Definition - Software that resides in a user's desktop or laptop as opposed to software located on a remote server. The necessary criteria for acquisition or disposition are presented in Tables 5.1. Acquisitions outside the criteria will only be supported when a waiver has been granted as outlined in Department Order #102.

Table 5.1 Client Software Selection Matrix

Category	Sub-Category	Standard
System Software	Operating System	Windows XP
	Driver	Windows Compatible
	BIOS	Windows Compatible
	Network Operating System	Windows XP
	Communications Protocol	IPX/SPX & TCP/IP
	Messaging Protocol	SMTP (Internet)
	DBMS	Access XP
	Virus Protection	McAfee TVD
	Programming Language	Visual Basic 6
	Application Software	Word Processing
Spreadsheet		MS Excel XP
Presentation Graphics		Power Point XP
Communications & Electronic Mail		GroupWise 6
Desktop Publishing		MS Publisher 2002
Project Management		MS Project Management 2002
Diagramming Program		VISIO 2002
Web Browser		Explorer 5.5

Server Software

Definition - Software that resides in a server and provides services to multiple users on the network. The necessary criteria for acquisition or disposition are presented in Tables 6.1. Acquisitions outside the criteria will only be supported when a waiver has been granted as outlined in Department Order #102.

Selection Criteria

Table 6.1 Server Software Selection Matrix

	Category	Standard
System Software	Operating System	Windows 2000 Advanced
	Network Operating System	Windows 2000 Advanced
	Communications Protocol	IPX/SPX & TCP/IP
	Messaging Protocol	SMTP (Internet)
Category	Sub-Category	Standard
	DBMS	Windows SQL 2000
	Virus Protection	McAfee TVD
	Programming Language	Visual Basic 6
Application Software	Word Processing	MS Word XP
	Spreadsheet	MS Excel XP
	Presentation Graphics	Power Point XP
	Communications & Electronic Mail	GroupWise 6
	Desktop Publishing	MS Publisher 2002
	Project Management	MS Project Management 2002
	Diagramming Program	VISIO 2002
	Web Browser	Explorer 6

IT Telecommunications Upgrade Standards

Building Wiring Systems (BWS)

IT Fiber and Copper

Accepted industry standard for Building Wiring Systems (BWS) currently include:

Copper Solutions:

Cable: (In-Side Plenum)

Criteria Category	Sub-Category	Pair/AWG	Jacket Color	Standard
Data	6	4/24	Blue	TIA/EIA-568-B.2-1 (550MHz)
Voice	5e	4/24	Grey	TIA/EIA-568-B.2-1 (400 MHz)

Connectivity:

Criteria Category	Sub-Category	Type	Color
Jacks & Inserts	Snap-in Module	180° Exit	
	Icons	Color Coded Designation	Data/Voice/Blank
Wallplates	Singe Gang Faceplace	4 Jacks	Fog White
Surface Mount Boxes	Quad	Four Module	Fog White
Patch Panels	Rack Mounted	Standard Density	
Patch Cords	Modular	3ft	
	Modular	7ft	
Terminating Blocks	Cross Connect	110 Block	Terminate 48 pair

Quick Reference:

Manufacturer	Category	Part No.	Package
Cable:			
Hitachi	6	30025-8BL3	1000 ft Spool
Hitachi	5e	38891-GA2	1000 ft Spool
Connectivity:			
	Jacks & Inserts:		
Ortronics	Tracjack Snap-in Midules	OR-TJ600	
Ortronics	Tracjack Snap-in Blanks	OR-42100002	Kit of 10 Blanks
Ortronics	Data Icons	OR-203262155	
Ortronics	Voice Icons	OR-203281154	
Ortronics	Blank Icons	OR-20323X156	
Ortronics	Wallplates:		
Ortronics	Single Gang Faceplate	OR-40300546	White Fog
Ortronics	Surface Mount Boxes	OR-40400031	White Fog
Ortronics	Patch Panels	PSD66U24	
Panduit	Patch Cords	UTPCH3	3ft
Panduit		UTPCH7	7ft
Ortronics	Terminating Blocks	OR-110ABC6050	48 pair in 50 pair footprint

Fiber Solutions:

Cable: (Backbone)

Criteria Category	Fiber Count	Size/Type	Max Attenuation (dB/km)	Gigabit Ethernet Distance
Singlemode	12	8.3/125SM	1.0/.075	5000/----- Meters
Singlemode	24	8.3/125SM	1.0/.075	5000/----- Meters
Multimode	12	50/125MM	3.5/1.5	600/600 Meters
Multimode	24	50/125MM	3.5/1.5	600/600 Meters

Connectivity:

Criteria Category	Style	Type of Adapter	# of Fibers
Distribution Panels	Rack Mount	SC Duplex MM/SM	96
	Surface Mount	SC Duplex MM/SM	24 Port
Connectors/Couplers	SM	Ceramic Sleeve, Blue	12
	MM	Phosphor Bronze Sleeve, Beige	12
Patch Cords	SM	Duplex SC	1 Meter
	MM	Duplex SC	1 Meter

Quick Reference:

Manufacture	Category	Part No.	Package
Cable:			
Corning	12 Strand SM	012RW5-14101A20	Per ft Spool
Corning	24 Strand SM	024RW5-14101A20	Per ft Spool
Corning	12 Strand MM	012CW5-14131A20	Per ft Spool
Corning	24 Strand MM	024CW5-14131A20	Per ft Spool
Connectivity:			
Distribution Panels			
Ortronics	Rack Mount	OR-625MMC-96PE1B	Kit
Ortronics	Surface Mount	OR-615SC224	Kit
Connectors/Couplers			
Ortronics	SM	OR-615LC6M6	Kit
Ortronics	MM	OR-615LCMM6	Kit
Patch Cords			
Ortronics	SM	OR-615D08001M99C	Single
Ortronics	MM	OR-6115D50001M99C	Single

Cable Management Solutions:

The ADC standard station drop is defined as 2 data & 1 voice connection. All station cables should connect directly to their respective IDF closet (home-runs). Future installations should plan for the following voice and data connectivity:

Station Drop:

Usage	Pairs	Type/Cat	AWG	RJ
Voice	2	UTP/5	24	11
100T/1G data	4	UTP/6	24	45

Riser Cables:

Fiber Optic: 24 12 strands of single-mode fiber per floor
 Copper: UPT/6 (Riser rated)

Building-to-Building:

Cables should be fiber optic cabling, at least 12 strands, single mode depending upon site-specific configuration and requirements, SC Type connectors, 850 or 1300nm.

Requests for new installation or upgrades will be evaluated against the above standards for local requirements.

SANITIZATION DOCUMENT

Manufacturer: _____

Model: _____

Serial Number: _____

Tag Number: _____

Procedure completed by _____
(Print name)

Sanitized on _____ using the following procedure:
(DATE)

_____ Use a Windows 98 boot disk with FDISK and FORMAT on it.
Boot off diskette and run FDISK

_____ Enable LBA and delete any partitions and create a new partition using maximum disk space available

_____ Format hard drive using switches /S/U

(Signature)

(date)

Distribution:

ATTACHMENT D
Department Order 102

SUPERSEDES

Department Order 102, Information Technology, supersedes Department Order 102, Information Technology, dated June 19, 2002

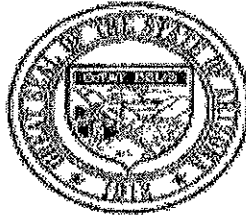
Director's Instruction 45, Automated Office Systems, dated June 1, 1997

Director's Instruction 173, Purchase of Hand-Held Computers, dated June 1, 2001

Director's Instruction 186, PC Sanitation, dated November 13, 2001

Director's Instruction 214, Internet Use, dated September 18, 2003

Director's Instruction 248, Security in the Use of Portable/Mobile Electronic Devices - Laptops, Cell Phones and Personal Digital Assistants (PDA), dated September 18, 2006



Governor Jan Brewer

ACCOUNT REQUEST FORM

To:	From:		
Fax:	Phone	Ext	
	:		
Phone:	Date:		
RE:	Pages		
	:		
<input type="checkbox"/> Add	<input type="checkbox"/> Delete	<input type="checkbox"/> Change	<input type="checkbox"/> Transfer Out

Information required for processing, incomplete forms will be rejected

Agency/Location

User ID

Name

EIN (Employee ID Number)

Phone **Ext**

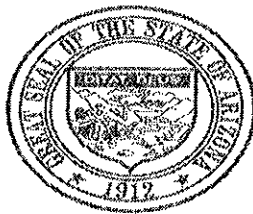
Additional Comments

Non Disclosure Form Attached

Verification Word Form attached

Manager Approval Signature: _____ **Date:** _____

Please fax completed forms to AIS at 602-542-0095



Governor Jan Brewer

DATA SHARING NON-DISCLOSURE

I have been made aware and understand that applicable laws, rules and ADOA directives bind all ADOA and non-ADOA personnel who have access. I agree to abide by all applicable laws, rules and ADOA directives, and pledge to refrain from any and all of the following:

1. Revealing data to any person or persons outside or within the agency who have not been specifically authorized to receive such data.
2. Attempting or achieving access to data not germane to my mandated job duties.
3. Entering/altering/erasing data for direct or indirect personal gain or advantage.
4. Entering/altering/erasing data maliciously or in retribution for real or imagined abuse or for personal amusement.
5. Using terminals, printers, and/or other equipment for other than work related purposes.
6. Using another person's personal data access control identifier (USERID) and password.
7. Revealing my personal data access control identifier and/or password to another person.
8. Asking another user to reveal his/her personal data access control identifier and/or password.

Appropriate action will be taken to ensure that applicable federal and state laws, regulations and directives governing confidentiality and security are enforced. A breach of procedures occurs pursuant to this policy or misuse of department property including computer programs, equipment and/or data, may result in disciplinary action including dismissal, and/or prosecution in accordance with any applicable provision of law including Arizona Revised Statutes, Section 13-2316.

My signature below confirms that I accept responsibility for adhering to all applicable laws, rules and ADOA directives. Failure to sign this statement will mean I will not be permitted access to ADOA produced media, computer equipment and software.

Name:

USER ID:

PRINT NAME

Signature:

Date:

Agency:

Phone:

Please fax completed forms to AIS at 602-542-0095



Governor Jan Brewer

Employee Verification Word Form

CONFIDENTIAL

Please think of one word easy for you to remember. The word can not be something easily associated to you. The word can not be a vulgar word. This word should not be revealed to anyone, including your supervisor or director.

Verification Word _____
(As an example BLUESKY)

PRINT YOUR NAME: _____

PRINT YOUR USERID: _____

NEW EMPLOYEES: After completing this form fax it and the non-disclosure form to **(602) 542-0095**.

CURRENT EMPLOYEES: If you want to change your verification word because you believe some one else knows your word, you may submit a new form. We will need your name, USERID and the new verification word to update your records.

The purpose of the verification word is to ensure that when you call the ADOA Help Desk, **(602) 364-4444**; they will reset your password to your USERID for **you** and not someone else. When you call, please tell them your name and your USERID. They will enter that USERID and the computer will give them additional information. The Help Desk person will ask you for your verification word. Please say the word you have provided (the one above). They will confirm that information with what they see, and if it matches/correct they will reset the password to your USERID. They will not reset the password if you give them an incorrect word. They will not provide additional guesses, clues or hints.

Please fax completed forms to AIS at 602-542-0095