OFFICE OF THE SECRETARY
1302 Pike Avenue, Suite C
North Little Rock, Arkansas 72114
Phone: (501) 682-3309 | Fax: (501) 534-3958
DOC.ARKANSAS.GOV

SECRETARIAL DIRECTIVE

SUBJECT: Information Technology Resources Policy

NUMBER: 2021-09

SUPERSEDES: ADC AD's 19-02, 16-14, 18-39, 17-04
ACC AD's 11-03, 14-20, 17-27 partial,
& APB AD 18-02

APPLICABILITY: All DOC Employees, Contractors, Volunteers, and others authorized to Utilize DOC Information Technology Systems

REFERENCE: A.C.A. § 25-19-102 (FOIA), 25-34-101, 25-43-105, 25-43-108, 25-43-403

APPROVED: Original Signed by Secretary Solomon Graves EFFECTIVE DATE: 7/15/2021

I. POLICY:

As the executive head of the Arkansas Department of Corrections (DOC), it is the responsibility of the Secretary of Corrections (Secretary) to administer the various rules, orders, or directives issued by the Department. The purpose of this directive is to establish guidelines for the acceptable use, security, maintenance, upgrade, repair, and disposal of the various forms of Information technology that are available to DOC employees, contractors, volunteers, and other individuals authorized to utilize that technology.

All supervisors are responsible for enforcing compliance with this policy. Violators will be subject to discipline as governed by the Department's Employee Conduct Standards & Discipline Secretarial Directive. Penalties may progress up to termination of employment, as well as initiation of criminal or civil action if appropriate.

II. DEFINITIONS:

A. Archive. A collection of historical records that primarily consists of records that have been selected for permanent or long-term preservation.

B. CD/DVD/BRD. Compact Disc, Digital Versatile Disc, and Blu-ray Disc are optical discs used for music, software, backup, and video storage.

C. Chief Technology Officer (CTO). The executive-level position tasked with the overall management and administration of Information Technology (IT) personnel, technological resources, programs, equipment, software, and technological issues within the DOC.

D. Criminal Justice Information Services Division (CJIS). A division of the United States Federal Bureau of Investigation (FBI) tasked with providing data and tools to law enforcement and intelligence organizations.

E. Communications Equipment/Systems. Includes, but not limited to, standard landline (phones) or Internet VoIP telephones, facsimile machines, electronic mail, network computer/server access, internet, and/or on-line services.

F. Computer & Electronic Equipment. Includes all personal computers (PC's), terminals, printers, network equipment and other computer-related equipment (smart or cell phones, tablets, media players, smart watches, speakers, laptops, thumb/flash drives, and other devices capable of storing computer files or software).

G. Copyright. Creative artist's control of original work or intellectual property; the legal right of creative artists or publishers to control the use and reproduction of their original works.

H. Data and System Security Classification (DIS SS-70-001). A framework applicable to all state agencies, including the DOC, under which data and systems are classified across the two spectrums of (1) data sensitivity and (2) data/system criticality. Once data and systems are classified, appropriate security measures (including personnel Security Clearance) measures can be applied. The data sensitivity levels are briefly summarized below:

1. Level A – Unrestricted. Open public data with no distribution limitations, anonymous access. May be anonymous access via electronic sources.
2. Level B – Sensitive. Public data with limited availability, but which requires a special application to be completed or special processing to be done prior to access.
3. Level C – Very Sensitive. Data only available to internal authorized users. May be protected by federal and state regulations. Intended for use only by individuals who require the Information while performing job functions.
4. Level D – Extremely Sensitive. Data whose disclosure or corruption could be hazardous to life or health.

I. Degauss. The complete removal of Information from a hard drive, not a specific technology for doing so. To de-magnetize or render the magnetic media or hard drive completely unusable.

J. De-Manufacturing. End-of-life disposition of electronic devices and computers; includes recovery of hard drives and chips with resale value, the removal of commodities, such as copper, aluminum, and gold for sale to scrap consumers, the removal and hazardous waste disposal of toxins and heavy metals, and the shredding or melting of materials that can be sold and manufactured into new products.

K. Encryption. The process of converting Information or data into a code designed to prevent unauthorized access.

L. FOIA. The Arkansas Freedom of Information Act gives Arkansan's access to public records and public meetings, with some exceptions. Under FOIA, the DOC must supply documents that are not exempt immediately if they are readily available. If requested records are in active use or storage, DOC must make every reasonable effort to supply disclosable documents, after redacting Information not disclosable, within three (3) business days.

M. HDD. Hard Disc Drives refers to storage drives with internal moving components or spinning discs.

N. Hotspot. An ad hoc wireless access point that is created by a dedicated hardware device or a smartphone that shares the phone's cellular data.

O. Information. The data, Information, and knowledge created, stored, accessed, or transmitted using computing resources.

P. License Agreement. A legal contract between two parties known as a licensor and a licensee. In a typical License Agreement, the licensor grants the licensee the right to produce and sell goods, apply a brand name or trademark, or use patented technology owned by the licensor. In exchange, the licensee usually submits to a series of conditions regarding the use of the licensor's property.

Q. Marketing and Redistribution (M&R). The Marketing and Redistribution Section of the Department of Transformation and Shared Services.

R. Multi-Factor Authentication. A method of accessing a system where a user is required to know at least two of the three following forms of identification:

1. Something you know such as a traditional ID and Password/Memorized Secret;
2. Something you have such as an enrolled key fob, cell phone, or email address on a different domain; or
3. Something you are such as fingerprint, iris pattern, facial structure, voice pattern, etc.

S. Mobile Devices. A portable, wireless computing device that is small enough to be used while held in the hand. May have an independent connection to the internet or DOC intranet. (i.e., Laptop, Smartphone, Tablet or Music Player).

T. Offender. Individuals under the custody or supervision of a division of the Department of Corrections, including but not limited to inmates, residents in a community correction center or reentry center, parolees, and probationers.

U. Password/Memorized Secret. A secret word or string of characters that is used for authentication to prove identity or gain access to a resource, sometimes referred to as an Access Code.

V. Protected Health Information (PHI). Any Information about health status, provision of health care, or payment for health care that is created or collected by a covered entity or business associate of a covered entity, as defined by the Health Insurance Portability and Accountability Act (HIPPA) and can be linked to a specific individual.

W. Security Clearance. A process that may include a law enforcement background check and may be combined with some form of biometric identification (e.g., fingerprinting).

X. Single-Factor Authentication (SFA). A process for securing access to a system, such as a network or website, that identifies the party requesting access through only one category of credentials. The most common example of SFA is Password/Memorized Secret based authentication.

Y. Solid State Drive (SSD). A storage drive with no moving components, only microchip-based storage.

Z. Surplus Computer/Electronic Equipment. Computer & Electronic components no longer in use by the DOC and which have residual market value.

AA. Universal Serial Bus (USB)/External Hard Disc Drive (HDD). HDDs that connect with the use of USB or other external cables and contain moving components or spinning discs.

BB. Thin Client. A simple (low performance) computer that has been optimized for establishing a remote connection with a server-based computing environment in which the server does most of the work, including launching software programs, performing calculations, and storing data.

CC. Virtual Private Network (VPN). A technology that provides a secure, encrypted connection from a remote site to the state network for access to state hosted applications.

DD. Warning Banner. A notice which a user sees or is otherwise referred to at the point of access to a system that outlines the expectations for users regarding acceptable use of a computer system and its resources, data, and network access capabilities.

III. GUIDELINES:

A. General

1. The DOC shall provide its staff with Information technology resources and infrastructure to enable completion of the DOC's operational responsibilities.
2. All Computer & Electronic Equipment in use at DOC facilities and offices are the property of the DOC and are to be used for authorized business only.
3. All purchases and acquisitions of Computer & Electronic Equipment, Communications Equipment/Systems, software, or other related technology items must be approved in writing by the Chief Technology Officer (CTO) or Designee and reported to Inventory Control.

4. Users have no expectation of privacy related to the Information entered, received, or transmitted on DOC equipment. Management has the authority and capability to monitor, track, and record all activities involving DOC equipment. Monitoring is not done to intimidate or harass, but to ensure proper use of computer resources. All Information created by DOC equipment is an asset of the Department.
5. The Secretary may direct Internal Affairs to conduct random security audits of computer resources to ensure compliance with this directive. DOC users must cooperate with Internal Affairs regarding all audit requests.
6. Donated Computer & Electronic Equipment become property of the DOC. Proposed donations must be reported in writing to the CTO for donation approval prior to receipt, in addition to reporting the donation to the Accounting section for proper asset recording per Accounting Control procedure of Accepting Gifts, Grants, and Donations for the DOC.
7. All maintenance, repair, upgrade, and modification of DOC Computer & Electronic Equipment is restricted to authorized DOC IT personnel or vendors only. No other maintenance, repair, upgrade, or modification work may be performed by any other individual without prior written authorization from the CTO or designee.
8. All materials (e.g., hardware, software, files, etc.) created, installed, or stored on DOC computers become the property of the DOC and are subject to being reviewed, read, or removed by management or IT personnel.
9. Any change in the original issued use of any Computer & Electronic Equipment must be reported to the IT Section for review and approval by the CTO or designee. Changes in utilization may require that the equipment be returned to IT to be reconfigured.
10. All computer users are responsible for the proper use and care of the equipment being used as outlined by this Policy. Users and their supervisors are responsible for ensuring that the user has sufficient knowledge to properly operate the hardware and software/applications being used to prevent damage to the equipment or to the integrity or accuracy of the data being accessed. Computers must be kept in a well-ventilated area.
11. Wardens, Area Managers, and those of a higher rank responsible for the supervision of staff shall ensure that the IT Help Desk is notified of changes in users and advise of problems or potential problems with the computers or their physical security.

B. Hardware

1. The placement of all computers and related equipment purchased with DOC funds shall follow the current Information Technology Plan.
2. Approval must be obtained from the CTO or designee prior to relocating computer equipment. Information Technology must be notified for inventory purposes, to obtain Information on cabling, and to avoid downtime due to triggering network port security.

   Note: The CTO must approve retention of Computer & Electronic Equipment by an employee changing duty stations.
3. Prior to being installed, computers must be configured with the appropriate DOC operating system image.
4. If Computer & Electronic Equipment is sealed, the seal must not be broken without direction from the IT Section.

C. Software

1. All software purchases must be approved by the CTO or designee to ensure compatibility. Software purchases will also be reviewed to determine how they improve the efficiency and effectiveness of the DOC.
2. Only software properly licensed to the DOC may be utilized on DOC computers. Requests to use shareware, free, or non-licensed software must be made to the IT Section for approval. The IT Section will review the software for a determination as to its usability and security for the purpose requested.
3. Making unauthorized copies of DOC owned software is illegal and prohibited.

IV. COMPUTER SECURITY POLICIES AND STANDARDS:

A. Network & Systems Security Generally

1. The CTO is responsible for developing and implementing DOC computer security policies and standards, subject to approval by the Secretary.
2. Information handled or created by DOC computer systems must be adequately protected against unauthorized disclosure, modification, or destruction. Proper management of computing resources and Information shall be enforced by ensuring appropriate protection and dissemination throughout their life cycles as well as by following all relevant standards, including those established by the Criminal Justice Information Services Division (CJIS), the American Correctional Association (ACA), the National Institute of Standards and Technology, the Division of Information Systems (DIS) the Health Insurance Portability and Accountability Act (HIPPA), and other applicable statutes, rules & policies as required.
3. Computer & Electronic Equipment shall be placed in locations that lessen the possibility of tampering by Offenders, visitors, unauthorized employees, or any other non-authorized individuals.

B. Warning Banner. Warning Banners are required on all DOC access points in accordance with DIS SS-70-003. The Warning Banner shall warn authorized and unauthorized users:

i. About what is considered proper use of the system;

ii. That the system may be monitored to detect improper use and other prohibited activity;

iii. That there is no expectation of privacy while using the system; and

iv. Of the penalties for noncompliance.

C. Digital Identity. In accordance with DIS Policies on Digital Identity Management and the FBI's CJIS standards, each user authorized to access DOC Information resources will be assigned a unique personal identifier to be used for authentication purposes. Authentication standards include either Single-Factor Authentication (SFA) or Multi-Factor Authentication (MFA). The following additional Information pertains to the standards associated with a digital identity:

i. Users are assigned an initial user account with an issued Password/Memorized Secret to access the DOC network utilizing the MFA standard. Once logged onto the network, users will be prompted and are required to change to a secret Password/Memorized Secret known only to the user;

ii. Standard account Password/Memorized Secrets must be changed at least once every ninety (90) days;

iii. Administrator account Password/Memorized Secrets must be changed every sixty (60) days, or as required by regulation, whichever is sooner;

iv. Password/Memorized Secrets must be at least eight (8) characters in length and be a mixture of upper alpha, lower alpha, numeric, and special characters;

v. Password/Memorized Secrets must not be reused within twenty-four (24) Password/Memorized Secret changes or the maximum allowed by the system if it is less than 24; and

vi. Password/Memorized Secrets must be protected by each user and not given to Offenders, visitors, other staff, contractors, volunteers, or other unauthorized individuals.

D. Endpoint Protection & Virus Scanning. All systems attached to the state network that are capable of supporting Malware Protection Software must have such installed and enabled. DIS shall maintain a list of approved Malware Protection Software. All Malware Protection Software must be monitored by IT staff, the State Cyber Security Office or authorized 3rd party. At a minimum, virus and spyware definitions will be updated weekly or as soon as feasible after a publisher makes such available. IT staff will be responsible for endpoint protection, virus/spyware scanning, and ensuring compliance with all relevant practices.

E. Personnel Security

i. The CTO shall implement an ongoing security training program that communicates the IT security policy to each user and promotes understanding of the importance of IT security. The training shall convey that IT security is to the benefit of the DOC and all its employees, and that all employees are responsible for IT security.

ii. The CTO will ensure current records of individuals authorized to access sensitive Information are maintained. Users who have access to privileged or sensitive Information shall not disclose that Information to any source except to authorized individuals and shall not disclose the Information for a purpose other than conducting approved DOC business.

iii. Human Resources and contracted vendors shall notify the DOC IT Helpdesk via email at DOC.it.helpdesk.@arkansas.gov when a user's employment is terminated so appropriate actions can be taken to secure the DOC network.

iv. The CTO will ensure that operations and maintenance personnel, such as vendors and other service providers, only have appropriate access to IT resources that are necessary to complete the job.

F. Physical Security

i. The CTO shall establish appropriate physical security safeguards and access controls to prevent unauthorized access to areas containing computer system hardware, network equipment, backup media, and other devices or physical elements required for proper operation of DOC computer systems.

ii. At a minimum, Offender accessible computers, Thin Clients, or other computing equipment shall not be installed or located in an office/area with a network accessible cable, computer, or other networked communications related equipment not designed and secured for Offender use.

iii. Offenders are prohibited from using any DOC computer that is connected to the State network or Internet unless authorized in writing by the appropriate Division Director. In such cases, device configurations must be secured per IT specifications. Access shall be restricted, secured, and used only for the project or purpose specifically authorized.

iv. Users shall be alert to and notify the IT Helpdesk of any attempts to compromise DOC systems or Information by unauthorized parties.

v. Mobile computing devices such as laptops, smartphones, tablets, flash drives, etc. must be secured from access by unauthorized users. This may be accomplished through the utilization of Password/Memorized Secrets, passcodes, biometric locks, Encryption, or device management tools.

vi. DOC personnel shall not store or transport any confidential Information on non-encrypted external storage media or devices.

vii. Computers, terminals, or other devices that provide access to business records or sensitive data shall be configured to automatically lock the system after a maximum of fifteen (15) minutes of inactivity.

viii. Equipment not owned by the DOC such as personal computers, software, electronic devices, or peripherals (including, but not limited to, smart watches, cellular phones, laptops, tablets, speakers, thumb drives, etc.) shall not be brought within a DOC correctional or residential facility, unless authorized by a Deputy Division Director or higher, or by a Warden during an emergency situation. A Warden may approve a vendor to bring a personal computer or electronic device necessary for that vendor to provide their service. The utilization of personal computers & electronic equipment by employees of the DOC's contract medical provider will be regulated by the Deputy Director for Health & Correctional Programs (Division of Correction) or the Deputy Director of Residential Services (Division of Community Correction). Personal devices shall not be installed, connected, or otherwise integrated with any DOC computer equipment without prior written approval from the appropriate Division Director or the Secretary or designee.

ix. Where feasible, computer displays should face away from windows and doors to minimize the possibility of Information being viewed by unauthorized persons. Doors to offices containing computers are to be locked when the user is absent, if practical. If unable to close and lock a door, users must ensure computers are not accessible by others upon leaving their office.

G. Disaster Recovery

i. The IT Section shall maintain internal policies and procedures that cover Disaster Recovery and Data Security.

ii. These policies must include procedures governing off site backups, data retention periods, and testing of all systems.

V. INFORMATION TECHNOLOGY USAGE

1. Appropriate network and user account guidelines include but are not limited to:

a. DOC personnel will only access computer accounts that have been authorized for their use. Users must identify computing work with their own names or other personal identifier such that responsibility for the work can be determined and users can be contacted in unusual situations.

b. Network and application user accounts and Password/Memorized Secrets shall never be shared.

c. DOC personnel will utilize accounts only for authorized purposes. This policy does not prevent informal communication, but accounts must not be used for private consulting or personal gain.

2. Examples of Appropriate and Inappropriate Usage

a. Appropriate Usage. In general, appropriate uses of technology may include but are not necessarily limited to:

i. Accessing the Intranet or Internet for work related research and Information gathering that may be necessary to complete job tasks;

ii. Utilizing applications that accomplish tasks and fulfill job functions; and

iii. Facilitating communication and collaboration between staff and/or other appropriate entities.

b. Inappropriate Usage. The following list provides general uses which are prohibited with respect to the privilege of using the Information technology resources of the DOC:

i. Interfering with the security or operation of computer systems, the efficiency of computer systems, or restricting or inhibiting other users from using the system;

ii. Vandalizing equipment, software, or hardware;

iii. Attempting to alter or gain access to unauthorized files or systems;

iv. Downloading or copying Copyrighted material or files, including music, to state computer systems;

v. Using technology in a way that interferes with an employee's assigned duties or otherwise inhibits DOC productivity;

vi. Using technology in a way that violates or infringes on the rights of any other person, including the right to privacy. Examples include publishing or displaying any Information or material that is slanderous, defamatory, false, abusive, pornographic, sexually oriented, obscene, inaccurate, profane, threatening racially offensive, otherwise biased, discriminatory, or illegal;

vii. Knowingly transmitting material, Information, or software in violation of any local, state, or federal law;

viii. Conducting any unapproved solicitation or public relations activities;

ix. Conducting any political activity;

x. Conducting any unauthorized purchases or any unapproved business activity on behalf of the DOC;

xi. Soliciting the performance of any activity that is prohibited by law;

xii. Engaging in any activity for personal financial gain, such as buying or selling of commodities or services with a profit motive;

xiii. Viewing, downloading, or sending pornographic or other obscene materials;

xiv. Visiting or participating in social media or chat rooms not designed for professional interactions specifically related to one's job;

xv. Using the system for the purpose of criminal intent, or any illegal purpose; or any purpose which violates policy;

xvi. Using or attempting to use unauthorized computer resources, monitoring tools, network programs/testers, packet sniffers, remote access devices, key stroke recognition technology, or remote-control equipment and software;

xvii. Masking or otherwise falsifying the user's identity;

xviii. Establishing unauthorized network services; or

xix. Otherwise using state property in a manner that would cause public embarrassment to the DOC, or any other state agency, department, or division.

3. Privacy of Information

a. The DOC reserves the right to monitor and log all network activity with or without notice, including email and all website communications, and therefore, users should have no expectation of privacy in the use of these resources. The DOC will not monitor email transmissions on a regular basis; however, the construction, repair, administration, and maintenance of electronic messaging systems may result in random monitoring of transmitted or stored messages.

b. Messages may be accessed and monitored during investigations into suspected violations of policy or law.

c. Supervisors or Managers may obtain access to data (including email) under their employee's control when necessary to conduct DOC business.

d. Any electronic record (including email) that serves to document the organization, functions, policies, decisions, procedures, operations, or other activities of the DOC may be considered

public record and subject to FOIA. Access to electronic records including email will be in accordance with FOIA guidelines.

4. Electronic Mail (Email). Email is considered a network activity. As such, it is subject to all policies regarding the acceptable and unacceptable use of Information Technology, to include the Encryption of sensitive Information. It is not confidential, unless specifically protected by statute or administrative rule.

a. Purpose

Electronic mail is provided to support open communication and the exchange of Information between staff and other authorized users that have access to a network. This communication allows for the collaboration of ideas and the sharing of Information.

b. Guidelines

1. DOC personnel assigned an email account are responsible for using their account in accordance with established guidelines and in a manner that does not interfere with their duties.
2. Electronic mail or Email is available for use on the DOC network or on a state issued mobile device using multi-factor authentication. Email access on personal devices is subject to approval by the Chief Technology Officer or Chief of Staff. Conducting state business on an approved personal device will subject work-related information on the device to FOIA requests.
3. Electronic mail accounts must include an Email Signature to identify the sender by name, position, division, facility, or office assigned, email address, and telephone number. If a telephone number is not assigned to your position, the facility or office main number shall be included. A fax number shall also be included if one is utilized for your position. Email signatures must also include the DOC Confidentiality Notice.
4. Email Signatures must not include any verbiage that is not expressly approved by this policy, such as images (except for the approved DOC logo), tag lines, quotes, inspirational messages, or other such extraneous statements. Exceptions are not permitted unless approved by the CTO or Designee or the Secretary or Designee. Below is an example of an approved Email Signature content:

   John Doe
   Parole and Probation Officer
   Arkansas Department of Corrections
   Division of Community Correction
   Area 13/Camden
   John.Doe@arkansas.gov
   P: xxx-xxx-xxxx
   C: xxx-xxx-xxxx
   F: xxx-xxx-xxxx

5. Confidentiality Notice: This email message and any attachments are the property of the State of Arkansas and may be protected by state and federal laws governing disclosure of private Information. It is for the intended recipient only. If an addressing or transmission error has misdirected this email, please notify the author by replying to it. If you are not the intended recipient, you may not use, disclose, distribute, copy, print, or rely on this email.

c. Specifically prohibited in the use of email is:

1. Use of cursive or hard to read fonts;
2. Use of font color other than blue or black;

3. Any activity covered by inappropriate use statements or other prohibitions as identified in this policy;
4. Knowingly sending, forwarding, or opening chain letters, viruses, hoaxes, etc.;
5. Knowingly sending, forwarding, or opening executable files (.exe) or other attachments unrelated to specific work activities;
6. Use of abusive or profane language;
7. Any use that reflects an unprofessional image or poorly on the DOC or the State of Arkansas; and
8. Photos, images, clips, inspirational messages, and backgrounds other than plain white.

d. Email Storage. System storage limits are determined per assigned account. Users shall receive system notices when server storage limits are approaching maximum capacity. Messages no longer needed must be periodically purged from the user's mailbox. Messages requiring retention must be kept and maintained for future inquiries. DIS retains all emails according to the Arkansas General Records Retention Schedule. All emails within the retention period are available through e-discovery for FOIA requests, investigations, and audits.

5. Internet/Intranet Guidelines

A. General. Through access to the Internet/Intranet, DOC personnel can utilize the many research and resource tools available online. These tools can aid in preparing reports or projects required by the DOC. All DOC network users who are authorized network users may access the Internet. However, web filtering software may restrict access to certain websites. Access to these sites is subject to approval by the appropriate Division Director or the Secretary and is dependent upon the business need.

B. Appropriate Usage of Internet/Intranet Access. DOC personnel shall not abuse internet/intranet access and are responsible for making sure they use this access correctly and wisely. Personnel should not allow use of the Internet/Intranet to interfere with their job duties.

1. Examples of Appropriate internet/intranet usage includes but is not limited to:

a. Accessing and distributing Information that is in direct support of the business of the DOC;
b. Providing and simplifying communications with other state agencies, entities, and citizens of Arkansas;
c. Communicating Information related to professional development or to remain current on topics of general DOC interest;
d. Announcing new laws, rules, or policies;
e. Encouraging collaborative projects and sharing of resources;
f. Accessing on-line services in the performance of official business; and
g. Subscribing to any non-governmental or non-correctional outside services, in the performance of official business.

2. Examples of Inappropriate Internet/Intranet usage includes, but is not limited to:

a. Viewing, downloading, or sending pornographic or other obscene materials;
b. Browsing or "surfing" the Internet for Information not related to official business;
c. Streaming unauthorized Audio/Video including music, movies, or other such content unrelated to work;
d. Furthering purposes that violate agency policy or local, state, or federal law;

e. Engaging in any activity for personal financial gain, such as buying or selling of commodities or services;

f. Disseminating or printing Copyrighted materials (including articles and software) in violation of applicable Copyright laws; and

g. Otherwise reducing productivity of the DOC.

6. **Wireless Security**

A. All technology, including wireless and related technology, must adhere to the DIS Wireless Security Standard SS-70-010, as well as the State Security Policy defined by ACA § 25-4-105 et. seq. including, but not limited to, the following:

1. General Requirements. All wireless infrastructure devices that are housed within DOC locations, connect to the DOC network, or otherwise provide access to sensitive Information must:

a. Abide by all applicable standards specified by DIS;

b. Be installed, supported, and maintained by the IT Section or an IT approved contracted vendor;

c. Use approved authentication protocols and infrastructure;

d. Use approved Encryption protocols; and

e. Maintain a hardware address (i.e., MAC address) that can be registered and tracked.

2. Security. All configuration parameters, such as Service Set Identifier (SSID), keys, Password/Memorized Secrets, etc. of Wi-Fi access points or bridges that can be changed from default manufacturer settings shall be changed from the default. SSID broadcast must be disabled. Where applicable, the new security setting should be complex. Open or unsecured wireless networks shall not be installed or available in any DOC location.

3. Wireless Managed Networks may exist on the DOC network if the following requirements are met:

a. An appropriate Warning Banner must be presented to authorized and unauthorized users of the managed wireless environment;

b. Wireless users must be given the opportunity to view any appropriate acceptable use policy as a part of user authentication;

c. The SSID must be changed to one which appropriately identifies the wireless managed network;

d. Appropriate audit logs containing IP address, login id, and logon/logoff date and time stamps must be maintained based on the Arkansas General Records Retention Schedule; and

e. Systems or applications which contain data that is categorized by DIS Data and System Security Classification Policy as being Level B – Sensitive, Level C – Very Sensitive, or Level D – Extremely Sensitive must have appropriate access controls (firewall rules, router access control lists, and similar measures) that disallow wireless users from directly accessing the system or application. Users of a managed wireless environment which require access to these systems or applications must use appropriate technology such as encrypted VPN, SSL/TLS, encrypted web pages, or similar authenticated and encrypted technologies to access these resources.

4. Use of Wireless Networking in a non-Hotspot environment must adhere to the following:

a. The SSID must not contain Information relative to agency location, mission, or name, except for open wireless networks. Wi-Fi equipment shall be configured for infrastructure mode only.

b. All wireless transmissions between DOC's managed wireless access point or bridge and clients shall be encrypted utilizing the Wifi Protected Access (WPA2) protocol at a minimum to

prevent unauthorized access to the state network. Wired Encryption Protocols (WEP) and WPA shall not be utilized.

c. Wirelessly transmitted data and credentials granting access to state resources are subject to DIS Policy, Remote Access, as well as any other applicable standards.

d. Routine searches for and disabling of rogue Wi-Fi access points to the state network must be completed.

e. Bluetooth wireless devices must be secured to the maximum extent possible between the devices involved.

VI. COPYRIGHT GUIDELINES

A. Purpose of Software Availability. The DOC shall provide utility and application software to enhance the efficiency and productivity of its employees. DOC personnel and other authorized users must honor Copyright laws regarding protected commercial software used by the DOC.

B. Compliance with Copyright Laws

1. Copyright laws do not allow a person to store copies of a program on multiple machines, distribute copies to others, or to alter the content of the software unless permission has been granted under the License Agreement.

2. Upon written approval by the CTO or designee or the appropriate division director or designee, users may download Copyrighted materials, but its use must be strictly within the agreement as posted by the author or current Copyright law.

3. Unauthorized use of Copyrighted materials or another person's original work/material is considered Copyright infringement.

4. All personnel and authorized users that utilize software owned by DOC or the state must abide by the limitations included in the Copyright and License Agreements entered into with the software providers.

C. Virtual Private Network (VPN) Guidelines

1. Authorization. Users must be granted authorization by the Secretary, the appropriate division director, or their designee to utilize VPN access to the state network. The IT Section will then provide access and configuration instructions to this resource in accordance with the authorization.

2. Use of VPN Service

a. It is the responsibility of those with VPN privileges to ensure that their VPN connection is not shared with unauthorized users. The VPN must be disconnected when it is not in use by an authorized user for the state network resources.

b. All computers must use the required endpoint protection software under the state tenant and have all current security-related operating system patches. Equipment and Software must be configured to comply with DOC and state security policies. It is understood that equipment used for VPN services are an extension of the DOC network.

c. VPN privileges may be revoked at any time, for any reason and for any length of time, including permanently.

d. A VPN is a "user managed" service. This means that the user is responsible for procuring internet service for remote use unless approval has been provided for a DOC provided Hot Spot.

e. VPN services are to be used solely for DOC business support purposes. All users are subject to auditing of VPN usage. Violations of VPN use may result in loss of certain privileges, services and/or disciplinary action.

VII. MOBILE DEVICES

A. Applicability. Mobile Devices include, but are not limited to, a variety of devices and accompanying media that fit the following classifications:

1. Mobile/Cellular Phones;
2. Smartphones;
3. Laptop/Notebook/PCs;
4. Tablet devices capable of storing agency data and connecting to an unmanaged network;
5. Backup Tapes;
6. MP4 Players;
7. Smartwatches; and
8. Recording Devices.

B. All DOC-issued Mobile Devices and their content remain the property of the DOC and are subject to regular audit and monitoring. All communications made on DOC-issued Mobile Devices may be subject to FOIA requests. Personal Mobile Devices authorized to be used for DOC business will be monitored by Device Management Software approved by the DOC. Personal Mobile Devices may not be used for DOC business nor granted access to the state network unless approved by the Secretary or designee or the appropriate Division Director, after consulting with the CTO or designee to ensure all security protocols are implemented.

C. Mobile Device Security Requirements. The IT section is responsible for configuration and issuance of all DOC Mobile Devices. The IT Help Desk shall be notified when a position that has an assigned mobile device has been vacated. Mobile Devices are assigned to a position number and shall stay with the position unless approval has been provided by the appropriate Division Director, CTO, Secretary or Secretary Designee. The mobile device shall not be reissued without assistance from IT to ensure proper configuration. DOC Mobile Devices are required to have the following:

1. Encryption;
2. A Password/Memorized Secret four (4) digits or longer in length;
3. The assigned user's state email account setup on the device, if applicable;
4. Protection by a firewall, except in instances where firewall technology is not available;
5. A Password/Memorized Secret established for encrypted backups of the device;
6. Apple Devices purchased by the DOC shall be enrolled in Apple's Business Manager Program. The Apple ID assigned upon enrollment must be configured with the employee's state email address or state alias address;
7. Applicable Mobile Devices must be enrolled and configured within the DOC's Mobile Device Management System (MDM); and
8. Location Services must be enabled on the device (if available).

D. Appropriate Use of Mobile Devices

1. It is the responsibility of Mobile Device end users to adhere to all DOC policies and procedures established for standard Information technology devices and network usage. Mobile Device use is considered an extension of the DOC network.
2. All Mobile Devices used to conduct DOC business shall adhere to all security protocols and should be utilized appropriately, responsibility, and ethically.
3. All end users of Mobile Devices must use reasonable physical security measures. Mobile Devices must be protected by a strong Password/Memorized Secret. Password/Memorized Secrets should never be shared. All DOC data stored on the Mobile Device must be encrypted using approved Encryption techniques.

4. The IT section will follow procedures to permanently remove data from DOC-owned devices once their use is no longer required.
5. In the event of a lost or stolen mobile device, the end user must notify their Supervisor immediately who will then notify the IT Help Desk. The device shall be remotely wiped of all DOC-owned data. If recovered, notification of the recovery shall be made to the Supervisor.
6. Devices are subject to any building restrictions on use or possession of devices at those locations.

E. Inappropriate Use of Mobile Devices

1. Mobile Devices may not be provided to Offenders for use, configuration, training, education, troubleshooting, or for any other reason excluding vendor provided Tablet devices designed and secured for Offender use.
2. The use of Mobile Devices to bypass any security configurations of DOC or state networks, applications, and databases will be deemed as an intrusion attempt. IT personnel will notify the appropriate supervisor for determination of appropriate action based on the Employee Conduct Standards and Discipline directive.
3. Mobile Devices may not be used to modify or reconfigure DOC owned hardware and/or software. This includes any reconfiguration without appropriate management approval.
4. Mobile Devices may not be used in a manner that violates DOC policy, procedure, or any applicable local, state, or federal laws.
5. Calls to state-issued Mobile Devices shall not be forwarded to a personal device unless approved by appropriate Division Director or Designee.

VIII. REMOVEABLE MEDIA

A. Purpose. Removable media are a well-known avenue for data loss and a source of malware infections. This policy section is to define standards, procedures, and restrictions for end users who have a legitimate business requirement to connect portable removable media to any DOC network or related technology resources. The purpose is to also minimize the risk, loss, or exposure of sensitive information maintained by the DOC and to reduce the risk of acquiring malware infections. This removable media section applies to, but is not limited to, all devices and accompanying media that fit the following device classifications:

1. Portable USB-based memory sticks, also known as flash drives, thumb drives, jump drives or key drives.
2. Memory cards in SD, CompactFlash, Memory Stick, or any related flash-based supplemental storage media.
3. USB card readers that allow connectivity to a PC.
4. Portable MP3 and MPEG-playing music and media player-type devices such as iPods with internal flash or hard drive- based memory that support a data storage function.
5. External hard drives.

B. Procedure. DOC staff may only use DOC authorized removeable media for work-related functions. Sensitive information generally should not be stored on removable media. If this is required for DOC work, the media device must be encrypted and placed only on officially registered removable media devices. Employees, contractors, and temporary staff permanently erase DOC specific data from such devices once their use is no longer required. All users agree to immediately report to his/her manager and IT any incident or suspected incidents of unauthorized data access, data loss, and/or disclosure of DOC resources, databases, networks, etc.

Department owned devices shall be encrypted and will be available for issuance by the IT department. Only encrypted devices shall be used with DOC equipment.

C. Enforcement. Removeable media that has not been encrypted by DOC IT staff and registered for use on the DOC network shall be refused connection by server policies.

IV. EOMIS GUIDELINES

A. Purpose. The electronic Offender Management Information System (eOMIS) is a web-based application used to electronically track Offender sentence, institutional, and community supervision records including, educational, physical health, mental health, dental, pharmacy, lab, consults, sex Offender assessments, Parole Board events, crime lab DNA verification, county jail backlog, Offender clemency and pardon applications, and other added modules developed to effectively maintain Offender Information.

B. User Account Compliance. The State of Arkansas and the DOC considers all Information and electronic data contained in the eOMIS to be confidential and sensitive in nature. All Information obtained from eOMIS is to be treated as confidential. Access to and use of such Information or data is subject to legitimate business needs and shall only be authorized for employees whose normal job duties require such access. At no time is such Information to be emailed or otherwise disseminated to unauthorized individuals, or individuals who are not approved by the DOC to view this Information. Authorization includes CJIS online certification with a finger-print based background check. Exhibiting malicious intent or a lack of confidentiality, professionalism, or integrity in the access or dissemination of eOMIS Information may result in an employee being found in violation of this policy and subject to disciplinary action, up to and including termination in addition to referral for possible criminal prosecution.

C. Release of Information. eOMIS Information considered available for the public shall be released by authorized DOC personnel only or made available to the public on the DOC website.

X. OFFENDER USE OF DOC INFORMATION TECHNOLOGY

A. Generally. The DOC provides Offenders access to certain approved Information Technology resources and equipment when deemed appropriate. Offenders have no expectation of privacy during use or access to these resources. All Offender use of equipment and resources shall be monitored and audited to ensure usage compliance. Each area with equipment and resources for Offender usage must have a Program Supervisor, who is responsible for monitoring Offender usage. The Program Supervisor should routinely check the files on computers to ensure files are not password protected and no unauthorized content is on the computer, etc. If the Program Supervisor suspects unauthorized activity or content, he/she should notify the Warden and IT for a computer audit. The same protocol should be followed with Thin Clients but IT can audit remotely if needed.

B. Security and Labeling. Computer & Electronic Equipment provided for Offender use shall be appropriately secured and labeled by the Program Supervisor. Labels must include the Program Name and language indicating that the computer is for Offender use. The label must be affixed to the monitor and computer cage.:

C. Offenders may only be permitted access to computer or electronic computing devices:

1. With a purpose approved by the appropriate Division Director;
2. Secured for Offender use by the IT Section (i.e., Thin Clients);
3. Assigned for a job, program, or for educational purpose;
4. That are properly labeled for Offender use;
5. That are vendor secured; or
6. That are purchased by an Offender through a DOC approved program/vendor, or through Offender or family leases.

D. Offenders shall not be permitted access to:

1. Computer hardware on the state network issued for staff, volunteers, contractors, etc.;
2. Email or other network resources;
3. Computers with access to Offender records maintained within eOMIS, ACIC/NCIC, AFIS or similar databases;
4. Printed reports with Offender records;

5. Mobile Devices not designed for Offender use;
6. Flash drives or other removable media; or
7. Any DOC business or personnel records.

XI. DISPOSAL/RECYCLING OF COMPUTER, ELECTRONICS, AND MEDIA:

A. Generally. Once Computer & Electronic Equipment is no longer able to support any functions within DOC, it will be marked as surplus, and readied for disposal. This condition may be the result of:

1. The PC (e.g., processor, memory, disks, etc.) is unable to run any necessary programs;
2. Aged hardware for which there is no viable replacement;
3. Failure of the hardware which results in the cost of repair exceeding the value of the system; or other conditions which make the operational usefulness of the equipment unable to support any DOC processing needs.

B. Computer & Electronic Equipment Recycling. DOC Asset Technicians are responsible for maintaining inventory control documentation of equipment purchased for DOC use. The inventory will contain the current location of the equipment and area of assignment until it is removed from DOC inventory.

1. All Computer & Electronic Equipment no longer in active service within the DOC shall be returned to the IT Section for reassignment or disposal.
2. After Computer & Electronic Equipment has been returned to the IT Section, it may:
   a. Be reassigned to other DOC personnel who need the equipment;
   b. Be used in a training classroom or reserved for other training requirements;
   c. Be held to maintain a back stock of used computer hardware and electronics to be used for parts harvesting for the repair, maintenance, and upgrade of other computers in use by the DOC. The back stock, should not exceed ten percent (10%) of the number of Computer & Electronic Equipment in active use within the DOC; or
   d. Readied for Disposal.

C. Surplus Computer & Electronic Equipment Handling. Before Computer & Electronic Equipment is disposed of in any manner, the IT Section will ensure that the hard drives are removed from the system for separate destruction. Computer equipment that has been designated as surplus will be cleared of data, and otherwise prepared for disposal within ninety (90) days of being marked as surplus.

D. Surplus Computer & Electronics Equipment Disposal Methods. At the end of the useful life of DOC Computer & Electronics Equipment, the IT Section will ready the equipment for disposal. Equipment will be inventoried to include Brand Name, Model Name and/or Number, Inventory Number, and Serial Number and placed in an outside storage container. When the container has been filled, the inventory list and disposal request forms will be submitted to the Accounting Section for disposal processing. The DOC may dispose of surplus computer equipment by any of the following methods:

1. Turn in to M&R for removal from the DOC inventory according to state procedures;
2. If equipment is refused by M&R, it may be sold to an outside commercial equipment recycler;
3. Other methods as approved by the DOC Accounting Section and in accordance with the Arkansas State Computer and Electronic Solid Waste Management guidelines; or
4. If all other means of recycling fail, then equipment may be disposed of in an approved landfill according to state and county regulations.

E. Media Sanitization and Data Loss Prevention. Recycled and Failed Hard Disc Drives will be Sanitized in accordance with NIST 800-88 (Guidelines for Media Sanitization) with the following categorizations:

1. Server, Shared Storage, Management Staff, and Video. These drives have been used for the listed purposes and have a very high probability of containing Level C – Very Sensitive data. These drives will not be repurposed in less sensitive, general operations or equipment.
2. General Staff and General Use Drives. These drives are used in standard computers for daily operations and are likely to store Level B - Sensitive data. These drives may be formatted and repurposed in other operations or equipment.
3. HDD and USB/External HDD Media. These drives will be sanitized by either Purge or Purge and Destroy methods, as described below:
    a. Purging will be accomplished by IT staff using the Degaussing machine located in the IT Warehouse.
    b. Purge and Destroy will be accomplished by IT staff using the Degaussing machine in the IT Warehouse and then physically removing the disc platters from the HDD.
4. SDD and USB/External Jump Drives. These drives will be sanitized by the following Purge and Pulverize method:
    a. Purge and Pulverize will be accomplished by IT staff using the Degaussing machine in the IT Warehouse and then bending the device or physically destroying it.
5. Legacy Storage/Floppy Discs and Tape Drives. These drives will be sanitized by the Purge and Incinerate method by using the Degaussing machine in the IT Warehouse and then sending the devices to an incinerator for destruction.
6. CD/DVD/BRD. These devices will be shredded by IT staff using a device with specific disc shredding capabilities.

F. Distribution of Revenues. Distribution of revenues from any equipment sales will be in accordance with the Arkansas Computer and Electronic Solid Waste Management Act A.C.A. 25-34-101 et seq.

VIII. ATTACHMENT:

Use of Information Technology Resources Consent Form

USE OF INFORMATION TECHNOLOGY RESOURCES CONSENT FORM

Employee Name: _____ Date: _____ AASIS #_____

I have read this Information Technology Resources Policy and agree to comply with all its terms and conditions.

The Arkansas Department of Corrections (DOC) provides access to technology resources and equipment as an instrument to complete job tasks.

I understand that the agency will not monitor e-mail transmissions, internet, or mobile device usage on a regular basis; however, through the construction, repair, performance of annual audits, and operations and maintenance, occasional monitoring may result in the random observation of user activity.

No Expectation of Privacy: By using DOC Technology Resources and Equipment, I waive all rights to privacy that I may have for such use. I agree that in order to ensure compliance with this policy, DOC representatives may monitor my use of the DOC technology resources including but not limited to email, email Archives, data or record Archives, voice transmissions, video transmissions, digital images, instant messages, email accessed from agency owned technology resources and equipment, mobile device usage, and application usage. I also understand that monitoring of Archives may occur even after my employment with the agency has ended.

The DOC makes no warranties of any kind, whether express or implied, for the service that is the subject of this policy. In addition, the DOC is not responsible for any damage(s) whatsoever which an employee may suffer arising from or related to their use of any agency electronic Information resources. Users must recognize that the use of DOC electronic Information resources is a privilege and that the policies implementing usage are requirements that mandate adherence.

Employee Signature: _____ Date: _____

Forward this form to the employee's HR representative for filing.