KAY IVEY
GOVERNOR

# State of Alabama
# Department of Corrections

Alabama Criminal Justice Center
301 South Ripley Street
P. O. Box 301501
Montgomery, AL 36130-1501
(334) 353-3883

JOHN Q. HAMM
COMMISSIONER

May 1, 2023

**ADMINISTRATIVE REGULATION NUMBER** 315

**OPR: INFORMATION TECHNOLOGY**

## USE OF INFORMATION TECHNOLOGY

## I. GENERAL

This Alabama Department of Corrections (ADOC) Administrative Regulation (AR) establishes and makes readily available to individuals needing access to Alabama Department of Corrections (ADOC) information technology, the rules of behavior that describe their responsibilities and expected behavior regarding ADOC information and information system usage.

## II. POLICY

Unauthorized use of ADOC Information Technology (IT) resources opens the ADOC and its data to risks including potential virus attacks, compromise of network technology and services, and legal liabilities. Effective security is a team effort involving the participation and support of every employee who deals with information and/or information technology. It is the responsibility of every IT user to know these rules and to conduct their activities accordingly. General rules of behavior are in place to protect the employee, ADOC, ADOC's IT resources, and data. It is the policy of the ADOC that users must:

A. Acknowledge that they have read, understand, and agree to abide by the ADOC established rules of behavior before gaining access to ADOC systems, applications, and data.

B. Report security-related issues and policy non-compliance to their immediate supervisor, manager, or ADOC Help Desk.

C. Conduct themselves professionally in the workplace and refrain from using information and IT resources, including telecommunications services, for activities that are not authorized under existing laws, regulations, or ADOC ARs and Standard Operating Procedures.

## III. DEFINITIONSS AND ACRONYMS

There are no definitions or acronyms prescribed for this AR.

## IV. RESPONSIBILITIES

This policy applies to all users of all information technology that are the property of ADOC. All users have an obligation to read, understand, and comply with the rules and standards included herein. Failure to abide by these standards may result in disciplinary action. Specifically, users are defined as:

A. All employees, whether employed on a full-time, part-time, or temporary basis by ADOC.

B. All contractors and third parties that work on behalf of ADOC.

## V. PROCEDURES

The following rules of behavior define the acceptable and non-acceptable use of ADOC IT resources including systems, devices, software, and internet communications that include email, instant messaging, and social media as directed by OIT Standard 660S1, *User Rules of Behavior*.

A. Prohibited Activities:

All ADOC users must understand the following activities are prohibited. The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

1. Activities that are illegal under local, state, and federal law.

2. Activities with adverse effects on agency operations and/or public confidence in the ADOC.

3. Activities in support of personal or private business enterprises.

4. Activities that are inappropriate or offensive to fellow employees or the public, such as hate speech or material that ridicules others based on race, creed, religion, color, sex, disability, national origin, or sexual orientation.

5. Activities toward the creation, download, viewing, storage, copying, or transmission of sexually-explicit or sexually-oriented materials.

6. Activities associated to gaining access to ADOC information or IT systems for which access has not been authorized.

7. Activities involved with the unauthorized transmission of ADOC operational data to an unauthorized recipient.

8. Activities toward the circumvention of system security or auditing controls.

9. Activities involving the introduction of unauthorized software onto ADOC systems.

10. Activities involving the introduction of unauthorized devices to the ADOC network.

11. Activities in disclosing, sharing, or attempting to acquire the passwords of others.

12. Activities with using or attempting to use the user accounts of others.

13. Activities involving sharing organizational data with Artificial Intelligence (AI) platforms such as ChatGPT, Jasper.ai, Chorus.ai, and YouChat.

B. Inmate Access to Technology:

1. The use of any ADOC computer resource by an incarcerated ADOC inmate is strictly prohibited, except for education and vocational training programs through ADOC, Alabama Correctional Industries (ACI), Ingram State Technical College, and the Alabama Prison Arts and Education Project (APAEP).

2. Users will not willfully, recklessly, or negligently divulge ADOC information to inmates, or in any way facilitate unauthorized access by an inmate to state computers, data or access to the Internet or Intranet.

3. No inmate under the control of the ADOC shall access the Internet using a computer, computer network, computer system, computer services, or information service, unless the inmate is under direct supervision and is taking part in an approved educational program that necessitates the use of the Internet.

4. Users authorized to use state owned computers capable of accessing the state Intranet or Internet within an area where inmates may gain access to the computer are responsible for the security of the computer and data/information contained within.

C. Internet Access and Use:

1. Access to the Internet is provided as a business and informational resource to support and enhance the capability of Internet users to carry out their job duties. Internet users are expected to handle their access privileges in a responsible manner and to follow all Internet-related policies and procedures.

2. The state reserves the right to access, monitor, or disclose all Internet activity as needed during monitoring, auditing, or responding to legal processes or investigative procedures.

3. Users do not have any right of personal privacy when using state-provided Internet services. All records created as a result of using Internet services are government records. As such, these records are subject to the provisions of state laws regarding their maintenance, access, and disposition.

4. Internet traffic is inspected and either blocked or allowed. Filtering policies define how security and access controls are applied to user's web requests.

    a. The following categories of Internet content present a threat to the security of state technology or have been considered not necessary for conducting official state business and shall therefore be blocked:

        (1) Games and Gambling;

        (2) Malicious Websites;

        (3) Nudity and Risqué;

        (4) Phishing;

        (5) Peer-to-Peer File Sharing;

        (6) Pornography; and

        (7) Proxy Avoidance.

    b. Any additional website(s) or category of sites not listed above may also be blocked if deemed a cybersecurity risk.

    c. Access exceptions may be granted to blocked websites for legitimate use. Each request requires a legitimate business need and written justification before IT Division personnel will consider for unblocking.

    d. Any request for exception that is denied based on security risk should be escalated through the proper authorization channels before appealing to the Director of Information Technology Division.

D. Email Usage:

To ensure the integrity and availability of email system resources all electronic communications are expected to comply with relevant federal and state laws as well as state policies and standards. Email shall be distributed, stored, and disposed of based on the data content in accordance with state information management requirements or ADOC Records Disposition Authority. Email content created, stored, transmitted, or received using state resources are the property of the state. Authorized personnel may access, monitor, or disclose email content for state business purposes or to satisfy legal obligations.

1. Email Encryption:

Operationally sensitive data and Personally Identifiable Information (PII) must be encrypted due to the unsecure nature of regular email. Office 365 encryption allows users to send secure emails. When in doubt about the sensitive nature of the email; encrypt it by using one of the below methods:

a. Encrypt an email by typing [encrypt] in brackets anywhere in the subject line of the email prior to sending.

b. Encrypting email thru Outlook can be done in a new email by selecting Options from the ribbon; then Permission; then Encrypt-Only. Once done, "This message is encrypted" is displayed near the top of email message.

c. Encrypting email thru Outlook Online can be done when creating New Message and then select "Encrypt".

2. Personal Use of State Email:

a. State email technology are to be used for business purposes in serving the interests of the government and of the people it serves; however, occasional personal use of state email is permitted. Users do not enjoy any right of personal privacy when using state email services.

b. Supervisors and managers are responsible for determining the reasonableness (frequency and duration) of personal use.

c. Personal email shall be deleted or saved separately from work-related email.

d. Users are permitted to include personal appointments in their Outlook or business calendar to help eliminate scheduling conflicts.

e. Users may store personal contact information with their business email contacts.

3. State Email Users Are Prohibited From:

a. Creation or distribution of any disruptive or offensive messages, including offensive (vulgar or pornographic) content or offensive comments about a person's race, gender, age, appearance, disabilities, political beliefs, or religious beliefs and practices. Employees who receive any email with this content from any state employee shall report the matter to their supervisor immediately.

b. Sending or forwarding remarks and/or images considered obscene, offensive, racist, libelous, slanderous, or defamatory.

c. Using an individual state email account to send or forward security advisories, terrorist alerts, or other official warning, alert, or advisory

messages to non- State of Alabama recipients unless approved by the ADOC Commissioner's Office.

d. Sending unsolicited email messages including junk mail, spam, or other advertising material to individuals who did not specifically request such material except in the execution of normal government information dissemination.

e. Posting to newsgroups or other social media using a state email address unless as part of official duties.

f. Using state email for personal or commercial ventures, religious or political causes, endorsement of candidates, or supporting non-government organizations.

g. Sending or forwarding chain letters or joke emails.

h. Misrepresenting or attempting to disguise their identity when sending email.

i. Sending messages using another person's email account (unless authorized to do so).

j. Intercepting messages destined for another person's email account (unless specifically delegated access to that person's account).

k. Unauthorized use, forging, or attempting to forge email header information or messages.

4. Auto-forwarding state email:

To preclude inadvertent transmission of inappropriate information onto the Internet, auto-forwarding shall not be used to send state email to an Internet, public, or private email address.

5. Mass email:

Material sent to group distribution lists must be relevant to the group being mailed and shall pertain to state business and/or serve the interests of state employees or constituents.

a. Message content/format:

(1) Message format may be text, Hyper Text Markup Language (HTML), or Rich Text Format (RTF) and should not include attachments unless approved.

(2) HTML or RTF format messages may contain artwork but shall be limited to a single page.

(3) Each message shall contain a signature block with the sender's name, departmental affiliation, office telephone number, and email address.

(4) Sender is responsible for all replies, responses, and complaints.

b. Message approval:

Approval authority for agency/organization-level groups (e.g., "ADOC – All Users and Facilities") shall rest with executive management.

E. Instant Messaging:

Instant Messaging (IM) is subject to many of the same threats as email (known security holes, information leaks, vulnerability to malware, etc.), and IM users are frequently the target of phishing attempts.

1. IM shall be used only for business communications (it is not provided for personal use).

2. IM shall not be used to communicate sensitive or confidential information.

3. IM file transfers shall be blocked for file transfers external to the organization (in Office 365 this is a global policy set by the tenant administrator).

4. IM is correspondence that creates a record that can be subpoenaed and used as evidence in litigation or regulatory investigations; therefore, IM correspondence shall be retained in accordance with applicable state data and record retention policies.

5. IM content, created, stored, transmitted, or received using state resources, is the property of the state.

6. Nothing in this policy shall be construed to waive any claim of privilege or confidentiality of IM content.

7. Authorized state personnel may access, monitor, or disclose IM content for any business purpose or to satisfy legal obligations.

F. Removable Storage Devices:

Removable non-volatile storage devices (Universal Serial Bus (USB) Flash drives, removeable hard drives, MEG-1 Audio Layer-3 (MP3) players, digital cameras, or recorders) have the same vulnerabilities as disk media (malware, data loss) but in greater capacity, could be used to infect an information system to which they are attached, could be used to transport sensitive data leading to potential compromise of the data, and are frequently lost or stolen. Careful attention to the security of such devices is necessary to protect the data they may

contain. For these reasons, the following requirements apply to the use of removable storage devices:

1. Possession of portable electronic storage devices in inmate living areas or use of such devices for personal needs is strictly prohibited.

2. No removable storage device shall be attached to an ADOC information system unless issued and approved by the IT Division.

3. Removable non-volatile storage devices shall be secured, marked, transported, and sanitized as required by state standards in the manner appropriate for the data category they contain.

4. Removable non-volatile storage devices shall, whenever possible, be formatted in a manner that allows the application of access controls to files or data stored on the device.

5. Sensitive or confidential data shall not be stored on any removable non-volatile storage device unless encrypted in accordance with applicable state standards.

6. Maintain physical security of removable storage devices. Report immediately the loss or theft of any device containing any ADOC data.

7. For approved removable media policy exceptions, users of removable media shall ensure:

    a. Removable media may not be connected to, or used, in personal or home computers.

    b. Data shall be copied or stored on removable media only by authorized users in the performance of official duties.

    c. Removable media containing sensitive information shall have an external label that is marked and dated.

    d. Media containing information shall be protected against unauthorized access, misuse, or corruption.

G. Software Licensing and Use:

1. The term "software" includes the program, media, and licenses for all operating technology, utilities, services, and productivity tools whether freeware, shareware, open source, off-the-shelf, or custom-developed without regard to the system(s).

2. All system users must use only properly licensed software and must use that software in accordance with the terms and conditions of the license agreement.

3. Users shall NOT:

   a. Copy, download, nor install unlicensed software.

   b. Install personally owned software onto state-managed computer technology.

   c. Install state-owned software on any non-state-owned computer technology, including home computers, unless specifically authorized in the software license agreement.

H. Social Media:

1. Employees shall not use their state email account or password in conjunction with a personal social media platform.

2. Users must understand that postings to social media platforms immediately become part of a public record.

3. Users shall not post or release proprietary, confidential, sensitive, PII, or other state government intellectual property on social media platforms.

4. Users shall not speak on social media platforms or other on-line forums on behalf of ADOC, unless specifically authorized by the ADOC Commissioner or the ADOC Public Information Manager.

5. Users may not speak on behalf of the State unless specifically authorized by the Governor.

6. Users who are authorized to speak on behalf of the ADOC or State shall identify themselves by the following when posting or exchanging information on social media platforms and shall address issues only within the scope of their specific authorization:

   a. Full Name;

   b. Title;

   c. Division/Facility; and

   d. Contact Information.

**I.** Network Access and Use:

1. Users shall not operate any program, script, command, or send messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the network.

2. Users shall not execute any form of network monitoring which will intercept data not intended for the employee's host unless this activity is a part of the employee's normal duties.

3. Users, including ADOC information security personnel, shall not conduct network, system, or application scanning unless:

    a. It is within their normal employment responsibilities to conduct such scanning, and

    b. Scanning of any network, system, or application is first coordinated with the IT Division Director or Network Operations Manager.

4. Users shall not conduct security breaches or disruptions of network communication.

5. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless within the scope of regular duties. Potential disruptions include, but are not limited to, port/internet protocol (IP) scanning, packet sniffing, or IP spoofing.

6. Users shall not introduce malicious software (malware) into the network or technology (e.g., viruses, worms, Trojan horses, logic bombs, etc.) within reason of user's control.

7. User shall not access, possess, or transmit material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

8. Users shall not engage in any inappropriate use of the Wireless Local Area Network (WLAN) Service . Inappropriate use includes, but is not limited to:

    a. Sending unsolicited mass email messages (spam).

    b. Engaging in any activity or device to disguise the origin of any transmission.

    c. Engaging in any activity such as hacking or port scanning.

    d. Engaging in forgery or impersonation.

    e. Using the WLAN Service to collect personal data or attempt to collect personal information about third parties without their knowledge or consent.

    f. Engaging in any activity that adversely affects the ability of other people or systems to use the WLAN Service or the Internet.

J. Streaming Media:

1. Users are permitted to utilize authorized streaming media services (such as YouTube, Vimeo, Microsoft Stream) on state owned devices for approved business purposes to fulfill job duties and responsibilities.

2. Users must have supervisor approval prior to uploading or downloading streaming media to ensure it does not distract or impede employee work productivity or consume large amounts of information system resources on the state network.

3. Users may access Microsoft Stream media with personally owned devices by logging into the web portal.

4. Users shall not utilize business critical information technology to view, upload or download streaming media on the state network.

5. Users shall not upload or redistribute copyrighted material without approval from the copyright owner.

K. Device Protection:

1. Physical Safeguards:

   a. Whenever leaving a computing device unattended, lock it such that a password or personal identification number is required to resume use.

   b. Unless kept in a locked room or restricted-access workspace, secure laptops using a cable lock or alarm. Attach the locking cable to an immovable or unbreakable object.

   c. If leaving a device out overnight, lock the entrance(s) to the room. If the room cannot be locked, then secure the device in a locked cabinet or safe.

   d. Never leave a portable device in view in a vehicle; do not leave devices in a vehicle overnight.

   e. Use privacy screens in public facilities or open, high-traffic environments to prevent "shoulder-surfing" when on-screen data needs to be kept private.

2. Lost Devices:

   Users shall immediately report the loss of any computer or data storage device to their immediate supervisor or IT Division Help Desk.

L. Personally Owned Mobile Devices (POMD):

1. Personal smartphones, tablets and other smart devices may only be connected to ADOC wireless network after getting facility/division management level approval via a signed ADOC Form 315-A, *Personally Owned Mobile Device User Agreement.*

2. Prior to initial use on the ADOC network or related infrastructure, the signed Personally-Owned-Mobile Device User Agreement will be forwarded to IT Division via the IT Division Help Desk.

3. Unauthorized use of mobile devices to back up, store, and otherwise access any ADOC related information/data is strictly forbidden.

4. IT Division reserves the right to refuse, by physical and non-physical means, mobile device connectivity to ADOC infrastructure.

M. Policy Compliance:

1. Regardless of role, all ADOC users must acknowledge that they have read, understand, and agree to abide by the rules of behavior before being authorized access to ADOC information and information technology. Electronic acknowledgement of this policy is acceptable and can be accomplished by logging into the ADOC security awareness training portal, navigating to the "Policies" section, and clicking the acknowledgement checkbox after reading the policy. https://www.mythreatadvice.com/policies

2. All ADOC users shall complete ADOC computer-based IT Security Awareness Training program within 30 days of being hired. ADOC IT Security Awareness Training is designed to provide users with baseline knowledge to securely operate ADOC IT systems. Topics covered in training include but not limited to:

   a. Data Retention;

   b. Data Security;

   c. Email & Messaging;

   d. Ethics;

   e. Insider Threat;

   f. Privacy;

   g. Social Engineering;

   h. Wi-Fi Security;

i. Social Media;

j. Personal Identifiable Information;

k. Password Security.

3. Annual IT Security Awareness Training is required to ensure users IT security knowledge remains current. Failure to complete annual IT Security Awareness Training will result in users access to ADOC IT systems being restricted.

N. Non-Compliance:

1. Any employee or contractor found to be in violation of the requirements of this agreement may face disciplinary action. This action could include termination of the agreement allowing the individual to access State IT resources on their POMD. The employee or contractor could also face criminal or civil action based on State and Federal laws regarding the care and use of protected health information (PHI) and (PII) data.

2. Any violation of this policy will be subject an employee to disciplinary action in accordance with ADOC Administrative Regulation 208, *Employee Standards of Conduct and Discipline*.

## VI. DISPOSITION

Any forms used will be disposed of and retained according to the Departmental Records Disposition Authority (RDA).

## VII. FORMS

ADOC Form 315-A, *Personally Owned Mobile Device User Agreement Form.*

## VIII. SUPERSEDES

This Administrative Regulation supersedes AR 315, *Computer Usage and Security Guide,* August 3, 1998, and any changes.

## IX. PERFORMANCE

A. State of Alabama Information Technology (IT) policies as defined by the Office of Information Technology (OIT)

B. Ala. Code (1975) Section 41-4-220 *et seq.*; Section 41-4-280 *et seq.*; and Section 41-28-1 *et seq*.

John Q. Hamm
Commissioner

**STATE OF ALABAMA**

**Personally Owned Mobile Device User Agreement Form**

## I. Authorized Use

Personnel eligible to accrue overtime or compensatory time are not authorized to use their Personally Owned Mobile Device (POMD) to conduct state business. Only state employees who are exempt under the Fair Labor Standards Act (FLSA) are authorized to use a POMD for state business. At the discretion of their employing Agency, the use of POMDs to access State of Alabama IT resources is allowed for authorized State employees and contract personnel under a state-issued contract (collectively "User").

## II. Personal Responsibility

The following are the responsibilities of each individual User using a POMD to access State IT resources. The user agrees:

1. Allow and install state-approved containerization software on their POMD before using device for state business purposes.

2. Any cost(s) associated with additional data usage, or the installation of applications deemed necessary by the Agency to ensure security and POMD management that are not covered by the Agency, are the responsibility of the individual User.

3. To promptly deliver the POMD, together with all passwords required to unlock the POMD and other information necessary to access State IT resources:

    a. When directed by the Agency for such purposes as may be deemed necessary for protecting State IT resources.

    b. Upon separation of service with the Agency for the purpose of wiping State data, deactivating State applications and any other action determined necessary to safeguard State IT resources.

4. Keep locator functions turned on, and security settings as specified by the Agency.

5. That only applications from authorized app stores will be installed on the POMD.

6. To use only vendor-supported operating systems (OS) on the POMD, and to update the POMD OS and security software when updates are provided by the vendor to keep POMD licenses and software at current vendor-supported version.

7. To immediately report to the hosting Agency the loss, upgrade, replacement, compromise, or theft of a POMD, and assist the Agency in any resulting investigation.

8. No changes shall be made to any agency-configured security settings without prior agency approval.

9. No modification of POMD functionality shall be made unless required or recommended by the hosting agency.

10. No device shall be utilized that is jail-broken, "rooted" or has been subjected to any other method of changing built-in protections.

11. To remove State data and State applications prior to disposal of POMD.

12. To follow the employee or contractor Agency's policies regarding POMD utilization if they are more restrictive or provide additional requirements; and

13. To consent to remote "wipe" of data, de-activation of State application or any other action necessary to protect State resources, including action which may result in loss of personal data.

## III. Security

User agrees to protect State IT resources from corruption or unauthorized access, to include, but is not limited to, the following:

1. Restricting use of the POMD to only themselves and those State IT resources specified in this policy.

2. Not divulging information that allows access to the POMD to anyone other than State IT resources specified in this policy.

3. Keeping State data segregated from personal data.

## IV. No Expectation of Privacy

User grants a waiver of privacy to personal data on their POMD only to the extent necessary to resolve any security or technical issue. User understands support personnel may access personal information incidental to an investigation or technical issue.

## V. Release from Liability

By accessing State information and application through a POMD, User agrees and expressly releases the State from any and all liability damage or loss of use of an employee's POMD to include personal data or information on the POMD. User expressly releases and holds the State harmless.

## VI. Consequences of Inappropriate Use

Any employee or contractor found to be in violation of the requirements of this agreement may face disciplinary action. This action would, at a minimum, include termination of the agreement allowing the individual to access State IT resources on their POMD. In addition, they may also face Agency or State Personnel disciplinary action. In extreme cases, the employee or contractor could face criminal or civil action based on State and Federal laws regarding the care and use of PHI and PII data.

## VII. Authority

This User Agreement form is promulgated under the authority of the Secretary of Information Technology in accordance with the Code of Alabama, Sections 41-28-1 through 41-28-8, (Act 2013-68).

## VIII. Acknowledgment and Agreement

By signing this document, I am agreeing to abide by each point listed above, and that I have read and understand the Policy governing this agreement form. I further agree to uphold the highest standards in using my personal electronic device. I understand that by failing to abide by this agreement that I will be subject to the consequences as defined in this form, along with any further disciplinary actions deemed appropriate by the state.

Employee Name: _____

Email: _____

Employee Signature:_____ Date:_____

*Deputy Commissioner/Division Director:*

Name: _____

Signature: _____ Date:_____