



**STATE OF ALABAMA  
DEPARTMENT OF CORRECTIONS**

**FOB JAMES, JR.**  
GOVERNOR

Research, Monitoring, & Evaluation  
Post Office Box 301501  
Montgomery, Alabama 36130-1501

**JOE S. HOPPER**  
COMMISSIONER

August 3, 1998

**Administrative Regulation  
Number: 315**

**OPR: Information Systems**

**COMPUTER USAGE and SECURITY GUIDE**

**I. General Policies**

**A. General**

**1. Definitions:**

- a. DOC – The Alabama Department of Corrections
- b. User – Any person utilizing DOC computing resources
- c. DOC Computing Resources – Any DOC owned or controlled hardware, software, networking device, service or product.

2. The DOC relies heavily on the use of electronic data processing systems and computers to meet its operational, financial, and informational requirements in an efficient manner. It is essential that its systems and equipment be protected from misuse, and unauthorized access. It is also essential that the DOC computers, and the data that they store and process, be operated and maintained in a secure environment.

3. All DOC employees and authorized users of DOC computer and network facilities are required to comply with the Alabama Computer Crime Act of 1985, the State of Alabama Acceptable Use Policy (which are included in this document as Annex A and B for

reference only), and the Computer Network Security and Acceptable Usage Policies in this document.

4. A user who intentionally and without proper authorization, directly or indirectly, damages or destroys any computer, computer system, computer network, program, or data, or causes any such acts to occur, will be subject to adverse action. In the case of DOC employees, such adverse action may include termination of employment. In cases where such activities violate State or Federal criminal statutes, violations (whether committed by DOC employees or others with no such connection to the DOC) may be reported to appropriate law enforcement authorities for investigation and prosecution.
5. A user who utilizes the DOC provided computer equipment, including network facilities, for any purposes other than for official DOC purposes, is guilty of misuse of state resources, and is subject to both DOC personnel action and appropriate criminal prosecution,
6. DOC management may, with prior evidence of misuse, both monitor and limit incoming and outgoing electronic messages to ensure compliance with all legal requirements and DOC policies. The unauthorized use of any DOC computer and network resources may be subject to termination of computer services, and other appropriate DOC personnel and State Code action.
7. All users of DOC computers must read this document and sign the Employee Consent Form in Annex C of this document. Any use of DOC computers with network capabilities by persons who have not signed the Employee Consent Form constitutes prima facie evidence of unauthorized use of DOC computer and network facilities, and will be subject to discipline or prosecution, or both, as specified in this policy.

**B. Securing DOC Owned Computer Resources**

All computer equipment, including personal computers, mainframe computer systems, software, files, and computer generated reports are assets of the DOC and must be protected from misuse, unauthorized manipulation, and destruction. These protection measures may be physical and/or software based.

**C. System Administrator Requirements**

All computer assets are assigned to a responsible party. Each application system, and its associated programs and files, are assigned a system

administrator who is responsible for ensuring that adequate controls and procedures are in place to protect the integrity of the resources. These controls include application design, testing, computer access security, and proper usage and disposal.

**D. Adherence to Terms of Software Licenses and Agreements**

All users provided access to DOC computers must adhere strictly to the terms, conditions, and limitations contained in the software licenses and agreements relating to computer software used on any DOC computer.

**E. Limitations on Use of DOC Computer Resources**

All DOC computer resources, including personal computers, mainframe computer systems, software, files, and computer generated reports may be used only for authorized purposes in support of official functions of the DOC.

**F. Information Classified for Reasons of National Security**

No information or computer programs classified for reasons of national security by the Department of Defense or other federal agencies may be stored, transmitted, or utilized on DOC computer facilities except in strict conformity with the requirements of the agency classifying the information or computer program. Users may obtain assistance from the DOC management in this regard.

**G. Consent to Monitoring to Confirm Unauthorized Use of DOC Computer Systems and Networks**

Any individual who utilizes any DOC computer resource consents by that use to monitoring of such use.

**H. Prohibition of Use of Social Security Numbers to Identify Records of Individuals**

Social Security Numbers will not be used to identify computerized records of any individual except to the extent that such use is permitted by the Privacy Act (5 U. S. Code 552a).

**I. Protection of Privacy of Employee Records**

The policies and procedures of the DOC will respect the privacy of employee records as defined in the Privacy Act (5 U. S. Code 552a).

**J. User Access of Computer Systems**

1. All users are held accountable for all actions performed on the computer systems with their log-on ID (i.e., user name and password).
2. Users are only to perform functions on the computer systems for which they are authorized and only to the extent that they have been authorized.
3. The following constitute a violation of DOC policy:
  - a. Deliberate, unauthorized attempts to access or use the DOC computers, computer facilities, network systems, programs, or data or the unauthorized manipulation of the DOC computer systems, programs or data.
  - b. Deliberate, unauthorized use of DOC facilities or equipment to access non-DOC computers.
  - c. Deliberate, unauthorized activity that causes DOC computers, computer facilities, systems, programs, or data to be accessed or used.

## **II. User Responsibilities**

### **A. General**

All users of DOC computing resources must bear certain responsibilities for assisting in the maintaining of security controls. Those responsibilities include the following:

1. All users are responsible for adoption and active support of security procedures including:
  - a. Keeping their network password confidential.
  - b. Reporting all known security exposures and violations to his/her supervisor or the DOC Information Systems Division; and
  - c. Using DOC computers and computer systems only in support of their authorized job responsibilities or consistent with the limitations of the permissions granted them (in the case of all users).

### **III. User Management Responsibilities**

#### **A. Definition of User Management**

User management are those persons who facilitate computer resources, issue user Ids and passwords, and are responsible for overseeing the use of computer systems.

#### **B. Responsibilities**

1. Reviewing and approving all requests for changing their employee's access authorizations;
2. Initiating security change requests to keep employees' security records current with their positions and job functions, including termination and transfers.
3. Reporting any known security violations to the DOC Information Systems Division.

### **IV. Security Administrator Responsibilities**

#### **A. Definition of Security Administrator**

The Security Administrator is a DOC designated individual responsible for both the security policies of all DOC computer/network resources and the DOC's internal compliance with the Acceptable Usage Policy.

#### **B. Responsibilities**

1. Providing basic security support for all systems;
2. Advising in the implementation of security controls on all systems, from the point of system design, through testing and production implementation;
3. Providing comprehensive information about security controls affecting system users and application systems;
4. Providing security support for all system users;
5. Maintaining the DOC Computer Security and Acceptable Usage Policy Document.

6. Serve as the DOC working contact with local, state, and federal agencies in instances of DOC employees violation of Security and Acceptable Use Policy; and
7. Report Security and Acceptable Usage Policy violations to the head of the DOC Information Systems Division.

## **V. Safeguarding of Computer Hardware**

The best rule to follow in safeguarding your hardware is to treat your computer resources as you would any piece of delicate equipment that you depend on. More specifically, do not allow the machine to be exposed to elements such as dust, smoke, and/or liquids that can easily harm the electronic circuitry and other sensitive items such as floppy diskettes or a hard disk.

## **VI. Safeguarding of Computer Software**

### **A. Copyright Laws/Proprietary Software**

1. All software must be used in strict compliance with the license or other agreement that sets out the terms and conditions of its use; all users must keep in mind that those terms vary.
2. Failure to comply with the usage restrictions contained in a software license or other agreement can result in DOC and/or personal liability and may result in disciplinary action. Federal and state criminal prosecutions are also a possibility.

## **VII. Safeguarding of Computer Data**

The best protection for your data is to lock it up. Store your storage media, reports, etc. in a secure place. If your computer does not have a lock, do not store sensitive data on the hard disk; use external media so that the media and data can be securely stored in a lockable cabinet.

## **VIII. Data Security**

### **A. General**

It is very important that all users of DOC computer equipment are aware of the importance of data security in the overall function of the Department. Unauthorized dissemination of DOC computer data could result in serious damage to the Department and could compromise the Department's ability to perform its primary functions of public security and inmate management. For these reasons, unless specifically approved otherwise, all data stored on any DOC computing resource will be for internal departmental use only.

**B. Employee Responsibilities**

No DOC employee shall provide any entity outside of the Department with any electronic data or printed reports containing information about any aspect of DOC operations without the approval of the DOC Commissioner or the DOC Public Information Officer. Failure to follow this procedure will be considered a violation of the Employee Conduct regulations as stated in DOC Administrative Regulation 207.

**C. Data Access by Inmates**

The use of any DOC computer or network device by a currently incarcerated DOC inmate is expressly prohibited. No employee will allow an inmate to access any aspect of the DOC network using his/her user name and password. Additionally, no employee will leave any DOC computer that is logged on to the DOC network unattended in the presence of an inmate. Any damage caused by an inmate accessing a DOC computer will be considered the responsibility of the employee whose user name and password is used to gain access.

**IX. Computer Networks and Configuration Responsibilities**

**A. General**

The DOC network is a valuable business resource that is available to the employees of the Department to assist them in the performance of their job. Due to the nature of electronic data networking, the potential for harm to the entire network by one errant component is significant. It is important for all users to understand that the network will function only if everyone follows a set of basic guidelines for network access and use. This requires all DOC network configurations (including all LANs and WANs) to be approved and the overall configuration maintained by the Information Systems Division.

**B. Definition**

The DOC network consists of approximately 500 nodes and provides data communications for operations, institutional, and administrative applications. The primary internal network is Ethernet and the only supported protocol is TCP/IP. Attachments to the Ethernet backbone shall be made only by DOC Information Systems personnel using previously approved components. All primary networking equipment will be considered to be the management responsibility of the Information Systems Division. No user shall move or modify any element of the primary

networking equipment without the permission of the Information Systems Division.

**C. Primary Networking Equipment**

The network consists of primary and secondary networking equipment. Primary networking equipment is generally those pieces of equipment that are seen by the network as a "whole", including:

1. Fiber optic and LAN cabling
2. Patch panels and premises wiring.
3. Transceiver taps and cables.
4. Active elements such as routers, bridges, repeaters, and gateways.

**D. Secondary Networking Equipment**

Secondary networking equipment includes equipment that is logically on the "user" end of a bridge or gateway, such as workstations and Local Area Networks (LANs).

**E. Lack of Privacy/Security of Certain Information on Networks**

Because of the many access methods, types of storage devices, backup routines, and nodal system administrator requirements, no data on any node should be considered private or secure. The network user is responsible for the integrity and security of files and transmissions.

**F. Network Address Assignments**

Only the information Systems Division will assign network addresses to any device on the DOC network.

**G. Inter-departmental applications, networks attachments, including LANs and WANs**

Any inter-departmental network applications, network attachments (including LANs and WANs) must be coordinated with the Information Systems Division. Failure to comply with this network policy will result in removal of the offending equipment from the network.

**X. Password Administration**

**A. Password Secrecy**

1. Passwords are to be kept confidential. Only the individual user to whom the log-on ID is assigned is to know the password.

2. Passwords are not to be programmed into a computer or recorded any place where someone may find them.
3. Disclosure of the password is a serious security violation and may result in loss of systems access privileges, and possible disciplinary actions.

#### **B. DOC Password Creation Guidelines**

1. When creating a password, it is important not to use one that may be easily guessed, like a common dictionary word or name of a relative or pet. The best passwords are purely random combinations of letters, digits, numbers, and punctuation.
2. Through the use of networking software, DOC will enforce the following password policies:
  - a. All passwords will be at least six characters in length.
  - b. All passwords will contain at least one non-alphabetic character. Acceptable non-alpha characters include numbers and special characters such as \$,&,#... etc.
  - c. All passwords will be changed every 90 days. The password policy will prevent the reuse of any of your previous passwords. In other words, once a password has been used, you can never use that same password again.

#### **XI. Dial-Up Access**

Access to the personal computers or mainframe computer systems via dial-up phone lines will be controlled by security systems to provide an acceptable level of protection from unauthorized entry. Access via dial-up connection will be implemented only by the Information Systems Division.

#### **XII. Computer Virus Protection**

The infiltration of destructive computer viruses has increased in recent years and prudent computer utilization demands protective measures. All workstations on the DOC network will have an anti-virus program installed. The DOC Information Systems Division will be responsible for assuring that the virus detection signatures are up-to-date. The presence of anti-virus software on every DOC computer does not eliminate the need for every user of the DOC computing resources to protect their system from potential infections. Remember, no anti-virus program will detect every potential virus, so each user must follow the established procedure of

never loading any program on their computer that is not approved by the Information Systems Division.

### **XIII. Obtaining DOC Network Services**

#### **A. LAN Access**

Every DOC workstation user will have access to the Local Area Network (LAN) at their site. The LAN will allow for the sharing of files and printers between users at that location, as well as allowing access to the local e-mail exchange. Access to certain DOC programs, such as the Institutional Apps, will still be controlled by the security system built into those programs.

#### **B. E-Mail**

DOC will be using Microsoft Exchange for its internal e-mail system. Every user who has a user account on the DOC network will have access to this internal e-mail system. Additionally, it is anticipated that users will have access to the statewide e-mail system, which will allow the exchange of messages with other State of Alabama governmental departments. Due to the increased security risks and the extra cost involved, the Information Systems Division will tightly control access to worldwide Internet e-mail

#### **C. Mainframe Access**

Access to the DOC mainframes and the ISD IBM mainframe will be controlled by the Information Systems. Only those users whose job functions require access will be allowed to use these systems.

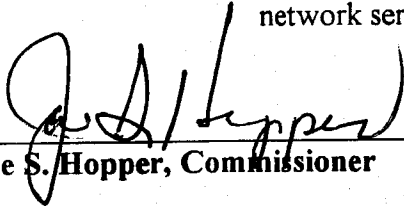
#### **D. Internet Services**

There will be some DOC employees whose job requires access to the increasing wealth of information available only through the public Internet. The Information Systems Division will only grant these employees' request(s) for public access. Upon approval, their name will then be entered in an approved list within the DOC network Firewall Security Computer, which includes all external access to the DOC network, and permits only named individuals to have public internet access.

#### **E. Request for DOC Network Services**

1. Employees must follow DOC procedures when seeking approval from the Information Systems division for any change in Network Services. No service will be provided without following these procedures. A sample of the Request for Access form is included in Annex D.

2. The DOC Information Systems Division will manage the connectivity to the requester's computer and the cost of necessary software/hardware will be handled in the normal manner for computer equipment purchases.
3. Only approved software and hardware will be installed for all network services.



---

**Joe S. Hopper, Commissioner**

**Annexes**

- Annex A Alabama Computer Crime Act
- Annex B Acts Constituting Offense Against Intellectual Property; Punishment
- Annex C Alabama Department of Corrections Employee Computer Policy Consent Form
- Annex D Alabama Department of Corrections Employee Internet Access Consent Form