Section-02 Information Management	OP-020701	Page: 1	Effective Date: 11/29/2018
Control and Use of Networks and Computers	**ACA Standards: 2-CO-1F-02, 2-CO-1F-03, 2-CO-1F-06, 4-4100, 4-4101, 4-4106, 4-ACRS-7D-05, 4-APPFS-3D-31**		
Joe M. Allbaugh, Director **Oklahoma Department of Corrections**	**Signature on File**		

Control and Use of Networks and Computers

The standards and guidelines for the use and care of computers and related networks are outlined in the following procedure. (2-CO-1F-06, 4-4100, 4-ACRS-7D-05, 4-APPFS-3D-31)

I. Standard Computer and Network Configurations

The Oklahoma Office of Management and Enterprise Services (OMES), Information Services Division (ISD), and the Oklahoma Department of Corrections (ODOC) Information Technology (IT) Unit has developed standards for configuration of computers and networks for ODOC. These standards provide the approved combinations of hardware and software. Any deviation from the standards must be approved by the OMES ISD, ODOC IT Unit. The standards for computer and software are posted on the ODOC web page (http://omes.ok.gov/services/information-services/policy-standards-publications). A hard copy of the standards may also be requested from OMES ISD.

II. Authorized Usage of Agency Computer and Networking Systems

A. General Guidelines

1. The user is authorized to perform all tasks that are consistent with the intended use of authorized software products.

2. Use of agency computer and networking systems for tasks of a personal nature is prohibited. All agency computer and networking systems are the property of ODOC and the assigned employee has no expectation of privacy in any personal item or information hosted or stored on ODOC systems.

3. Non-agency owned software or hardware shall not be used on agency owned equipment unless exempted by prior approval of the deputy chief of Operations and supported by a letter from the affected senior staff member. Prohibited products include:

   a. Animated screen savers, animated graphics packages, stock market or news “ticker” programs;

   b. Any commercially licensed products or “freeware” not approved by OMES ISD, ODOC IT Unit; and

   c. Personal hardware (e.g., personally owned computers, printers, scanners, USB drives/storage, cell phones/PDAs, digital players) or other hardware or software attached to an ODOC computer or network.

4. The types of files to be maintained on computers are:

   a. Standard software supplied by the OMES ISD, ODOC IT Unit or purchased from the authorized standard software list;

   b. Data files maintained by authorized applications software;

   c. Application software developed by the OMES ISD, ODOC IT Unit; and

   d. Application software approved by the OMES ISD, ODOC IT Unit.

5. The standard hardware and software configurations are developed by the OMES ISD. All computers and networking equipment shall conform to these configurations. The OMES ISD, ODOC IT Unit must approve any deviation from the standard configurations.

6. Games are not authorized on ODOC computer systems and shall be removed or disabled.

B. Security and Privacy of Information (2-CO-1F-06, 4-4101, 4-ACRS-7D-05)

The State of Oklahoma has published a document covering information security policy, procedures and guidelines. This document can be found at http://www.ok.gov/OSF/documents/StateOfOklahomaInfoSecPPG_osf_12012008.pdf. All ODOC computer and networking systems shall adhere, where applicable, to this document.

Security of computers and software are the responsibility of the user site. The user site, at a minimum, shall provide for the following:

1. Reasonable protection of computer equipment from theft and vandalism;

2. Prevention from unauthorized usage and tampering of equipment, including loading unauthorized software or games;

3. Prevention from unauthorized disclosure, copying, modification, or tampering with data and copyrighted programs;

4. Confidentiality of assigned passwords and changing of compromised passwords; and

5. The Central Human Resources Unit will notify the OMES ISD through the PeopleSoft alert system, when employees resign or are terminated, in order to allow OMES ISD, ODOC IT Unit to wipe clean each computer to prevent possible compromise of ODOC information. Region/facility/unit heads must notify the OMES ISD, ODOC IT Unit when employees are reassigned duties that do not require computer access.

C. Backups

1. System developers and maintainers are responsible for the backup of the systems under their control. These backup methodologies shall be submitted to the OMES ISD, ODOC IT Unit for review and approval. After initial approval by the OMES ISD, ODOC IT Unit, the developer/maintainer shall review backup methodologies annually and the result of the review shall be submitted to the OMES ISD, ODOC IT Unit.

2. Users should contact the OMES ISD, ODOC IT Unit for assistance in developing a backup methodology for their critical information not backed up by other means. It is the user's responsibility to ensure this information is protected.

III. Network (Wide and Local Area – WAN/LAN)

The OMES ISD, ODOC IT Unit shall control all network devices (e.g., routers, switches, firewalls, wireless access points, etc.). Employees shall not adjust or change the settings of any network device without the approval of the OMES ISD, ODOC IT Unit. No device/system (e.g., network, PDA, computer, sensor, camera, etc.) shall be connected to the network without the approval of, and coordination with, the OMES ISD, ODOC IT Unit.

IV. Training (4-4101)

Annual training will be provided by the Training Unit in accordance with OP-100101 entitled "Employee Development." Additional training may be provided through on-the-job training, Human Resources Development Services Division (HRDS) or other Oklahoma State government sponsored courses, vendor courses, seminars and Career Tech courses.

V. Access

A. Access to systems will be requested by completing an "IT Services and Systems Authorization Access Request (IT SAAR) Form," including all and any adds, moves, and changes to access. The IT SAAR form can be obtained by contacting the PSD Service Desk and requesting access.

All completed IT SAAR Forms must be emailed to itsecurity@doc.ok.gov and accompanied by a Service Case number provided by the helpdesk. All new employees should receive an IT SAAR form as part of the documents provided in employee onboarding packets.

B. The types of access that can be requested are:

1. Email Access
2. Computer Access
3. Cell Phone
4. PeopleSoft
5. CSI/InfoShare
6. Offender Management System
7. COMIT
8. VPN (Remote access)
9. Internet Access
10. File Access

11. Offender Banking

12. Document Imaging Software

13. SharePoint

14. Other Agency Specific Software

VI. Maintenance and Problem Reporting

A. Routine Care

1. Users should prevent damage caused by liquids, food, other foreign objects, and impact damage (dropping the system or dropping objects onto the system).

2. Users should turn off their computers at the end of each workday unless instructed to do otherwise by the OMES ISD, ODOC IT Unit.

B. Trouble Shooting

1. If the user cannot resolve the problem locally, the OMES ISD, ODOC IT Unit help desk at the agency's administration office should be contacted at (405) 521-2445, or by case submitted utilizing the on-line help desk system (http://servicedesk.ok.gov) , or by submitting an email to PSDservicedesk@omes.ok.gov

2. If the problem cannot be resolved over the telephone or by remote access, the appropriate support person will be sent to the user's site. Depending upon the type of problem encountered, the defective device may be sent to the OMES ISD, ODOC IT Unit administrative offices. Time estimates to resolve the problem will be provided by OMES IT personnel.

3. End users are not to attempt to reinstall software, hardware, or other devices unless directed to do so by OMES ISD, ODOC IT Unit personnel. Field sites will not contract with local vendors to attempt resolution unless this has been coordinated with the OMES ISD, ODOC IT Unit.

VII. Passwords

Passwords are a primary means of identifying and authenticating users. Employees shall not share individual user passwords. Sharing password(s) compromises the integrity of critical systems (i.e., electronic health records, offender management system, etc.). Any access to the system or activity

performed on the system using a password is attributed to the owner of the password.

Supervisors may request, through their chain of command, access to ODOC user accounts. If approved, OMES ISD, ODOC IT Unit will facilitate access to the account(s).

A. Strong Passwords

Where possible, “strong passwords” shall be used. Minimum requirements for strong passwords are:

1. Minimum of eight characters in length;

2. Contains at least one number;

3. Contains at least one symbol (!, #, $, etc.);

4. Contains at least one case change;

5. Does not contain common words; and

6. Does not contain, and is not based on, any personal information such as family names, birthdays, addresses, etc.

Further guidelines for strong passwords can be found in the state information security guidelines:

https://www.ok.gov/OSF/documents/StateOfOklahomaInfoSecPPG_osf_12012008.pdf.

B. Security and Maintenance of Passwords

1. User identification and passwords should be memorized. If written down, user identification and passwords shall be secured at the same level as the information being accessed.

2. As a security measure, passwords shall be changed every 60 days. If the information system does not enforce the changing of passwords, the user is responsible for changing the password every 60 days.

C. Laptops, PDA’s and Other Electronic Devices

1. Some systems and environments do not support a system administrator recovering information if the password is lost. An example of this is the password assigned by a user for encryption of information on a PDA or removable storage. These user

identifications and passwords shall be written down and secured by designated personnel. The user identifications and passwords shall be made available to authorized ODOC personnel upon request. The OMES ISD, ODOC IT Unit has a safe that can be used for storing passwords.

2. OMES ISD, ODOC IT Unit personnel shall assign passwords for encryption of ODOC information on laptops/PCs, PC and server administration, centralized computing environments and other agency wide applications.

VIII. Printers

Printers shall be purchased using the statewide printer contract with a minimum of a one year support contract. Multifunction copier/printers will be leased/purchased using the statewide contract.

IX. Oklahoma Correctional Industries (OCI) Standards

A. Hardware and Software Configurations

1. Customer requirements may deviate from standard combinations of hardware and software.

2. Applications specific to the support of manufacturing, data processing, and agriculture may be developed using software suited to those tasks.

3. The OMES ISD, ODOC IT Unit shall review all applications prior to purchase for compatibility and interoperability with agency standards for networking and telecommunications.

B. Network Maintenance and Security

1. OMES ISD, ODOC IT Unit staff will install and maintain all Oklahoma Correctional Industries (OCI) network devices and will provide help desk support for all OCI users. OCI may use inmates in the creation and maintenance of databases, processing of information and maintenance of all OCI computer equipment. OCI staff will supervise all such inmate activity.

2. Security procedures specific to the operation of the OCI Network will be implemented by OCI.

X. Annual Evaluation

The OMES ISD will evaluate information systems annually to ensure progress toward defined goals and objectives are being met. (4-4106)

XI. References

Policy Statement No. P-020700 entitled “Oklahoma Department of Corrections Information System”

62 O.S. § 45 Oklahoma Statute, Sections 45.1 through 45.10 “Oklahoma Program Performance Budgeting and Accountability Act”

XII. Action

Senior/executive staff is responsible for compliance with this procedure.

The deputy chief of Operations is responsible for the annual review and revisions.

Any exceptions to this procedure will require prior written approval from the agency director.

This procedure will be effective as indicated.

Replaced: Operations Memorandum No. OP-020701 entitled “Control and Use of Networks and Computers” dated October 25, 2017

Distribution: Policy and Operations Manuals
Agency Website