Section-02 Information Management	**OP-020701**	**Page: 1**	**Effective Date: 11/30/2021 Revision-01 dated: 01/12/2022 Revisions on pages 1, 6, 7, 8, 9, and 10**
Control and Use of Networks, Computers and Kiosks	**ACA Standards: 2-CO-1F-02, 2-CO-1F-03, 2-CO-1F-06, 5-ACI-1F-01, 5-ACI-1F-02, 5-ACI-1F-06, 5-ACI-1F-07, 4-ACRS-7D-05, 4-APPFS-3D-31**		
Scott Crow, Director Oklahoma Department of Corrections	**Signature on File**		

Control and Use of Networks, Computers and Kiosks

(Revision-01 dated 01/12/2022) The standards and guidelines for the use and care of computers, kiosks and related networks are outlined in the following procedure. (2-CO-1F-06, 5-ACI-1F-01, 4-ACRS-7D-05, 4-APPFS-3D-31)

I. Standard Computer and Network Configurations (5-ACI-1F-01, 5-ACI-1F-02)

The Oklahoma Office of Management and Enterprise Services (OMES) Information Services Division (ISD) and the Oklahoma Department of Corrections (ODOC) Technical Services and Operations (TSO) 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 and the ODOC TSO unit. The standards for computer and software are posted on the OMES-ISD 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. (5-ACI-1F-01, 5-ACI-1F-02)

II. Authorized Usage of Computers 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 owned computers and networking systems for tasks of a personal nature are prohibited. All agency-owned 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. Personally-owned software or hardware will not be used on agency-owned equipment unless exempted by prior approval of the chief technology officer and supported by a letter from the affected executive/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 TSO 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 TSO 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 TSO unit; and

   d. Application software approved by the OMES ISD, ODOC TSO unit.

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

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

B. Security and Privacy of Information (2-CO-1F-06, 5-ACI-1F-02, 5-ACI-1F-07, 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 computers and networking systems will adhere, where applicable, to this document.

Security of computers and software are the responsibility of the user site. The user site, at a minimum, will 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 and the ODOC TSO unit to reimage each computer to prevent possible compromise of ODOC information. Division/facility/unit heads must notify the OMES ISD and the ODOC TSO 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 will be submitted to the OMES ISD and the ODOC TSO unit for review and approval. After initial approval by the OMES ISD and the ODOC TSO unit, the developer/maintainer will review backup

methodologies annually and the result of the review will be submitted to the OMES ISD and the ODOC TSO unit.

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

IV. Training (5-ACI-1F-07)

Annual training will be provided by the Training unit in accordance with OP-100101 entitled "Training and Staff 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 CareerTech courses. (5-ACI-1F-07)

V. Access (5-ACI-1F-02, 5-ACI-1F-06)

A. Access to systems will be requested through the OMES help desk system. (5-ACI-1F-02)

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

1. Computer Access

2. Email Access

3. PeopleSoft

4. All offender management system

5. Internet Access

6. Offender Banking

7. SharePoint

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 and the ODOC TSO unit.

B. Troubleshooting

1. If the user cannot resolve the problem locally, the OMES ISD help desk 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. 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 unit personnel. Field sites will not contract with local vendors to attempt resolution unless this has been coordinated with the OMES ISD.

VII. Passwords

Passwords are a primary means of identifying and authenticating users. Employees will 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 unit will facilitate access to the account(s).

Further guidelines for strong passwords can be found in the state information security guidelines located at this link.

A. Security and Maintenance of Passwords

1. User identification and passwords should be memorized.

2. As a security measure, passwords normally will 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.

B. Laptops and Other Electronic Devices

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 removable storage device. The user identifications and passwords will be made available to authorized ODOC personnel upon request.

VIII. Printers

Printers will 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. Employee Kiosks (Revision-01 dated 01/12/2022)

Standards and guidelines for the use and care of the kiosks will be in accordance with this procedure and OP-021001 entitled “Oklahoma Department of Corrections Internet Standards.”

A. Kiosks

1. The kiosks will be made available to staff in facility administrative areas to provide access to commonly used online portals for ODOC. These networks are secured via WPA2 network security password protected connections.

2. Kiosks will remain plugged into an electrical outlet.

3. The kiosks will remain in the area of the state owned wireless access points. All kiosks will be in approved locations and may not be relocated without the permission of the chief of Technical Services.

B. Kiosk Features

1. The kiosk is a tablet PC that is secured in a custom built kiosk.

2. The application provides access to the following applications directly from the kiosk touch screen:

a. Office 365;

b. Learning Management;

c. Inside the Wire (SharePoint);

d. UpKeep request portal;

e. IT Service Desk; and

f. Time clock (TCP).

3. "Interactive Kiosk User Guide" (Attachment A, attached) is the kiosk user guide provided.

4. Kiosk content is managed by the office of the public information manager. Any requests for additional content added to the kiosk display, will be submitted through their chain of command and to this office.

C. Kiosk Maintenance

1. Kiosk Maintenance

a. The kiosk requires very low maintenance. The screen should be cleaned with an approved electronics cleaner used on computer monitor(s).

To clean the kiosk screen, use a screen cleaning wipe or a soft, dry, lint-free cloth. When necessary, you can dampen the cloth with one of the following: water, isopropyl alcohol (IPA) solution 70% or less, or eyeglass cleaner. **Never use glass cleaner or other chemical cleaners.**

b. The kiosk has a "self-healing" feature that will restart the computer in the event it freezes up or stops working. If the kiosk fails to recover from this event or is observed to not be working correctly, please notify the office of chief of Technical Services by emailing TechnicalServices@doc.ok.gov with the following information:

(1) Facility;

(2) Kiosk location; and

(3) Description of the issue.

D. Kiosk Accountability

1. The office of Technical Services will approve designated locations at each facility for assigned kiosks. It is the responsibility of the facility head to ensure the kiosks are located in the approved locations and

appear to be in working order.

2. The kiosk location will be identified on the facility inventory. In the event a kiosk requires relocation, a request will be submitted to and approved by the office of the chief of Technical Services, who will arrange the relocation.

3. The kiosks will be added to the "Weekly Administrative Staff Tour Log" (OP-130107, Attachment A), which requires a weekly check of location and functionality by the facility head.

X. 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 will 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 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.

3. Inmates will not be involved in any troubleshooting or maintenance of computers.

XI. Annual Evaluation (5-ACI-1F-01)

The OMES ISD will evaluate information systems annually to ensure progress toward defined goals and objectives are being met. Results will be provided to chief of Technical Services.

XII. References

Policy Statement P-020700 entitled “Oklahoma Department of Corrections Data System Management”

(Revision-01 dated 01/12/2022) OP-021001 entitled “Oklahoma Department of Corrections Internet Standards”

OP-100101 entitled “Training and Staff Development”

(Revision-01 dated 01/12/2022) OP-130107 entitled “Standards for Inspections”

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

XIII. Action

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

The chief of Technical Services 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: OP-020701 entitled “Control and Use of Networks and Computers” dated May 27, 2020

Distribution: Policy and Operations Manuals
Agency Website

(Revision-01 dated 01/12/2022)

Attachments	Title	Location
Attachment A	“Interactive Kiosk User Guide”	Attached
Attachment A	“Weekly Administrative Tour Log”	OP-130107