	Illinois Department of Corrections **Administrative Directive**	
Number: **01.05.105**	Title: **Use and Security of Computers and Computer Systems**	Effective: **4/1/2022**

Authorized by:	*[Original Authorized Copy on File]* **Rob Jeffreys** Director
Supersedes:	01.05.105 effective 6/1/2018

Authority: 730 ILCS 5/3-2-2	**Related ACA Standards:** 5ACI-1F-01
Referenced Policies: 01.05.103	**Referenced Forms:** DOC 0434 – Incident Report

I. POLICY

The Department shall control the acquisition and use of computer hardware and software to preserve the investment in the equipment, protect the integrity of data maintained by the equipment and establish department-wide guidelines for access to computers, devices and networks.

II. PROCEDURE

A. Purpose

The purpose of this directive is to ensure the proper acquisition and use of computer hardware and software.

B. Applicability

This directive is applicable to all correctional facilities, programs, and parole services within the Department.

C. Facility Reviews

A facility review of this directive shall be conducted at least annually.

D. Designees

The Chief Administrator and above may delegate stated responsibilities to another person or persons unless otherwise directed.

E. Definitions

1. Hardware - the physical equipment associated with data processing. This shall include, but not be limited to, stand-alone equipment or equipment attached to a local area network (LAN), such as computers, monitors, multifunction printers, USB drives, Personal Data Assistants (PDA), etc.

2. Software - the programs and applications used to direct the operation of a computer.

F. General Provisions

All State-owned computers, mobile hotspot devices and related hardware and software shall be used for official business purposes only. Personal or unauthorized use of equipment may result in disciplinary action up to and including discharge.

1. **Hardware**

   a. All computer hardware shall be acquired through the Department of Innovation and Technology (DoIT).

      (1) Requests for computer hardware shall be submitted in accordance with Administrative Directive 01.05.103.

      (2) Requests shall be approved by the Chief Information Officer (CIO) prior to being submitted to DoIT.

   b. Caution shall be used in and around areas containing computer hardware.

      (1) Hardware is susceptible to damage from excess heat and should not be operated in areas in excess of 85 degrees.

      (2) Extreme caution shall be taken if eating or drinking is allowed while using hardware.

      (3) Consideration shall be given to the placement of hardware to ensure equipment is placed on a safe and stable surface.

   c. Surge suppression equipment shall be utilized on all computer hardware; either through a protected circuit or through a plug-in model where the hardware is plugged directly into the surge suppression device.

      NOTE: Multiple computer hardware devices may be protected by an individual surge suppression device so long as the maximum amperage rating of the suppression device and circuit is not exceeded.

   d. Computer hardware shall not be removed from the facility without the written approval of the CIO or DoIT.

      NOTE: Portable devices, including, but not limited to, laptops and USB drives, may be exempt from this provision as approved by the Chief Administrator and CIO. PDAs and mobile hotspots shall be approved through the Office of Telecommunications.

   e. The LAN Administrator or other appropriately designated staff shall notify DoIT of any desired movement of computer equipment, excluding portable devices, using a service request submitted to the CIO.

      (1) DoIT staff must perform the equipment move unless instructions are provided to local staff by DoIT.

      (2) Appropriate inventory and location information must be documented by DoIT.

   f. All computer hardware damage and malfunctions shall be reported to the DoIT Customer Service Center (CSC).

2. **Software**

   a. No unauthorized software shall be copied or maintained on departmental equipment without the approval of the CIO and DoIT.

      (1) All software shall be obtained through DoIT.

NOTE: Software developed, provided or utilized by approved vendors and contractors may be purchased by the vendor or contractor, but shall be authorized and installed by DoIT.

(2) Requests for software shall be submitted in accordance with Administrative Directive 01.05.103.

b. Custom software shall not be developed without prior written approval of the CIO.

c. Approved custom software created by ISU may be included on the Department's Approved software list and distributed to facilities upon their request, provided the software is approved by DoIT.

NOTE: All custom software may be audited by authorized personnel at any time.

d. DoIT must document, maintain and distribute approved software to the local LAN Administrator.

e. The CIO shall ensure all data stored on Department computers is backed up and stored accordingly by DoIT.

f. All sensitive applications, such as those containing criminal history, shall be password protected.

3. **Internet and Networks**

a. Access and usage of the Internet, including access via a State-owned mobile hotspot device shall be for Department business only and shall be limited to the performance of specific assignments where the Internet is determined to be the only or best source of information to complete the assignment. The following uses of the Internet shall be prohibited:

(1) The use of games; and

(2) Personal use or general browsing unrelated to official duties.

b. All computer Internet access shall be approved by DoIT and obtained by submitting a service request to the CIO. Internet access through a PDA or mobile hotspot device shall be approved through the Office of Telecommunications by submitting a Telecom Service Request (TSR).

c. Only authorized computers may be connected to the LAN.

(1) Communication between a computer and any other computer, mainframe or LAN is prohibited, unless the computer is approved and equipped to do so by DoIT.

(2) LAN access shall be approved by DoIT and obtained by submitting a service request to the CIO.

4. **Data Security**

a. All computers containing sensitive or confidential information shall require password protection to prevent unauthorized access.

(1) Passwords shall be issued to staff individually. The use of group passwords

shall be prohibited, unless otherwise approved for computer-based training applications, including annual cycle training and ethics training, as approved by the CIO.

(2) Employees shall not use another employee's password or attempt to log on to an application for which authorization and password has not been obtained from management.

(3) Employees shall keep passwords confidential. To prevent unauthorized access, passwords shall:

(a) Never be written down;

(b) Be changed monthly; and

(c) Be easy to remember, yet difficult to guess.

(4) Employees shall report a compromised password immediately to the CSC and document the incident on an Incident Report, DOC 0434, and forward to their immediate supervisor. The DOC 0434 shall be forwarded to the Investigations and Intelligence Unit.

(5) The Chief Administrator shall submit a service request to the CIO to ensure DoIT is notified of any employee's change in employment status that may require computer access to be removed or changed. Changes in status may include termination, suspension, retirement or transfer.

b. Operating Systems and Configurations

(1) Changes to operating systems, configurations, system images or log-in scripts shall only be made by DoIT.

(2) Service requests for changes of operating systems or configurations shall be approved by the CIO prior to being submitted to DoIT.

c. Computer Viruses

(1) The CIO shall ensure each computer has antivirus software installed and enabled.

(2) All computer viruses shall be immediately reported to the CSC so corrective action may be taken to isolate and remove the virus before other computers can be infected.

(3) All computers shall be rebooted at least weekly to ensure system and security updates are automatically updated and installed.

d. All data, either in digital or paper format, containing sensitive or confidential information shall be:

(1) Produced and distributed in a secure manner;

(2) Stored in a secure location; and

(3) Shredded or disposed of by other appropriate and secure methods when retention is no longer required.

NOTE: Individual in custody related information shall not be taken out of the facility without written approval from the Chief Administrator.

5. **Individual in custody Use of Computers**

a. Excluding approved kiosks, individuals in custody shall only be permitted to use state-owned hardware or software, as approved, for educational purposes through the Office of Adult Education and Vocational Services (OAEVS) or for Correctional Industries work assignments and training.

b. The state-owned computer or device shall:

(1) Have system configurations and images that limit connectivity to specific authorized, predetermined software or web-based applications.

(2) Have any email, chat, instant messaging or peer-to-peer sharing deactivated.

NOTE: For online-based courses that require an email address for login, the email address and password shall be entered by OAEVS staff. Computer usage shall be monitored closely by OAEVS staff to ensure login passwords remain unobtainable to individuals in custody.

c. individuals in custody shall only access those computers and devices designated for Individual in custody use. Individual in custody access to staff computers shall be strictly prohibited.

6. **Use of Personally-Owned Computers**

a. Employees may not use their personally-owned computers or devices to access systems that must be audited and are controlled by Administrative Directives without the approval of the CIO and DoIT.

NOTE: Personally-owned external storage drives and devices may be used with written authorization from the Chief Administrative Officer. The external storage drives and devices shall only be used for official business, and the user shall ensure the automatic virus scan of the drive or device is not interrupted prior to use.

b. All work-related information residing on personally-owned computers or devices is the property of the Department and may be seized or audited by authorized personnel at any time.

c. The Department shall not be liable for any loss or damage of personally-owned computers, software or related equipment.