State of Indiana Indiana Department of Correction	Effective Date	Page 1 of	Number
	12/1/2020	6	04-05-109

POLICY AND ADMINISTRATIVE PROCEDURE
Manual of Policies and Procedures

Title
COMPUTER CONTROL

Legal References (includes but is not limited to)	Related Policies/Procedures (includes but is not limited to)	Replaces: New
11-8-5-2	02-03-106 04-05-102 04-01-101 04-05-103	

I. PURPOSE:

The purpose of this policy is to establish guidelines for the control of computer technology, to include but not limited to, computing devices, hardware, and individual computer components for the Indiana Department of Correction.

II. POLICY STATEMENT:

It is the policy of the Indiana Department of Correction (IDOC) to control and supervise the issuance, asset management, use, storage, and disposal of IDOC information technology (IT) hardware (i.e., computers, computer components and network equipment) in a safe and secure manner.

III. DEFINITIONS:

For the purpose of this policy and administrative procedure, the following definitions are presented:

A. AUTHORIZED USER: An IDOC employee, contractor, intern, volunteer or other agent of the State who is authorized at a technical level to administer and support/maintain State computing IT systems or is authorized at an end user level, to have access to and use State computing IT systems and telecommunications technology systems for business purposes on behalf of the State of Indiana.

B. COMPUTER: An electronic hardware device for storing and processing data, typically in binary form, according to instructions given to it in a variable program.

C. COMPUTER ROOM/CAGE: A secure location approved by the managing officer for storage of computers and hardware. This location shall have at minimum a single door and a high security lock. Offenders shall not be permitted to enter into the computer room/cage.

D. DIRECT SUPERVISION: The frequent, nonscheduled, direct, and unimpeded personal observation and contact between one or more IDOC staff members or other authorized individuals and offenders using authorized computing devices for approved pro-social, treatment, education, career technical, law library and industrial program tasks, assignments, duties, and/or activities. For the purpose of this specific definition, the use of IDOC surveillance cameras does not constitute direct supervision.

E. HARDWARE: The tangible, material parts of any IT device or system including desktop computers, laptops, tablet personal computers, keyboards, speakers, printers, central processing units (CPU), disk drives, servers, switches, routers, cable, fiber, etc.

F. INDIANA OFFICE OF TECHNOLOGY (IOT): The Indiana Office of Technology is the shared services agency in Indiana State Government which provides core IT services to all Executive Branch agencies.

G. INFORMATION SECURITY OFFICER (ISO): The technical staff member of IDOC that, in collaboration with the Indiana Office of Technology, Executive Director of Technology Services, and other IDOC technical staff members, is responsible for the security oversight of IDOC's IT system assets by establishing appropriate system asset security standards and risk controls to identify, develop, implement, maintain and support security processes across the IDOC IT resources and to respond to system asset security incidents.

H. INTERMEDIATE DISTRIBUTION FRAME: A cable rack that interconnects and manages telecommunications wiring between a main distribution frame (MDF) and workstation devices.

I. MAIN DISTRIBUTION FRAME: A primary, centralized cable rack that interconnects and manages the telecommunications wiring between itself and any number of intermediate distribution frames (IDF) and connects private and public lines coming in to a building with the internal network.

J. PORTABLE COMPUTING DEVICE: Any mobile electronic computer instrument or mechanism that allows a person to move from place to place and use or access IT services, products, and resources. Portable computing devices include air cards, laptops, tablet personal computers, smartphones, and other similar handheld mobile electronic instruments or mechanisms.

K. SOFTWARE: The intangible computer programs, procedures, algorithms, related data, and associated documentation stored in an IT device or system, that could be licensed intellectual property or open source, whose purpose is to provide the instructions for the operation of a data processing program or system. Examples of software include middleware, programming software, system software and operating systems, testware, firmware, freeware, retail software, device drivers, programming tools, and application software.

L. SYSTEM ASSETS: Computer hardware, telecommunications hardware and systems, digital devices such as digital copiers and facsimile machines, software, networks, the internet, IT information or data and/or IT services or IT resources that are made available by IDOC or IOT to authorized users and are necessary to conduct State government business and support the IT requirements of the IDOC and, therefore, must be protected by the appropriate security requirements to ensure business continuity

IV. PROCEDURES:

A. General Computer Security

1. All employee/staff use of computers, hardware, software, portable computing media, and portable computing devices shall be in accordance with Policy and Administrative Procedure 04-05-102, "Internet, Electronic Mail, and Online IT Service Use."

2. When any authorized user assigned a desktop or laptop computer leaves the physical proximity of their work area, the authorized user shall secure the computer to prevent unauthorized access to the device or its data/information, using one or more of the following methods:

   a. Log off all accounts, including the computer and/or network account;
   b. Lock the computer by using an approved password protected screensaver;
   c. Lock the computer by using operating system level workstation locking;
   d. Shut the computer down; and,
   e. For laptop computers, physically secure the system to prevent removal.

3. Offender access to IT hardware, software and system assets capable of accessing inmate, employee, victim, security, operational or any other sensitive or confidential IDOC information, data or records is strictly prohibited, in accordance with Policy and Administrative Procedure 04-05-104, "Offender Access to IT."

4. All offender access to IDOC IT hardware and software shall be limited to pro-social, treatment, educational, career technical, law library, and industrial program purposes through IDOC approved client systems.

5. All damaged computers, computer parts, and hardware shall be removed from service and disposed of in the appropriate manner as required in Policy and Administrative Procedure 04-01-101, "Fixed Asset Management." IOT owned equipment shall be returned to their control for repair or disposal.

6. Vendor provided players/tablets shall be controlled by the issued vendor. These devices shall have security measures installed on the device and/or the vendor's network, as mandated by the ISO or designee.

7. Staff shall not move any stationary computer, hardware, portable computing media and/or computing devices without authorization from the managing officer or designee.

8. Any computer, hardware, software, portable computing media or portable computing devices possessed by inmates without the proper approval as defined in Policy and Administrative Procedure 04-05-104, "Offender Access to Information Technology," shall be confiscated as prohibited property. The prohibited property shall be stored in a secured manner in such a way that access to the prohibited property is limited to the local facility investigator or managing officer.

9. All visible and readily accessible data cable under twenty (20) feet from a floor level shall be secured in rigid conduit to prevent tampering.

10. All IT network hardware, to include MDF and IDF servers and switches, shall be maintained in a secured computer room/cage with access limited to IDOC IT staff members and other individuals authorized by the managing officer.

B. Computer Identification

All computers and portable computing devices shall be issued an asset tag and/or identification tag/number.

C. Key Control

Key access to all computer rooms/cages shall be designated as restricted keys in accordance with Policy and Administrative Procedure 02-03-106, "Key Control."

D. Computer Inspection

1. At minimum, each facility shall conduct a random inspection of at least ten percent (10%) of authorized staff computers and all non-network computers within the institution. This inspection shall be conducted biannually and include the following:

    a. Search for stored and/or written down usernames and passwords;
    b. Staff members leaving unlocked computers accessible to offenders;
    c. Conducting a visual inspection of the work area for unauthorized hardware; and,
    d. Visually inspecting computers and hardware for tampering

2. A summary report of the computer inspection shall be completed by January 10th and July 10th annually. Each summary report shall reflect inspection of a different 10 percent (10%) sample of staff computers, as checking the same staff computers of the previous summary report is not acceptable. The completed summary report shall be forwarded to the managing officer/designee for review and, upon completion of the review, shall be submitted to the Executive Director of Technology Services. The appropriate facility IT staff member shall maintain the completed summary report on file for review by the respective regional operations manager.

E. Computer Storage

All computer hardware, when not in use, shall be stored in a secure room/cage designated by the managing officer or designee. Any IOT provided computer assets that are not actively in use shall be turned in to reduce associated monthly charges.

F. Removal of Computers

1. Computers, hardware, and devices removed from service and/or disconnected shall be secured in the institution's designated computer room/cage until salvaged or placed back in service. This includes computers, hardware and devices removed from service and/or disconnected for construction projects, staff reallocation or the termination of any facility program.

2. Offenders shall not be allowed access to inoperable IDOC system assets that are decommissioned, salvaged, repurposed, or physically moved from one location to another unless under direct supervision by a staff member.

3. All unused computer components (e.g., keyboards, mice, speakers, monitors, patch cable, power cords, HDMI cable, USB cable, and display port cables) shall be secured in the designated computer room/cage

G. Inventory

Each facility shall conduct an annual physical inventory of all computers and associated hardware each fiscal year. This inventory includes any computers provided by the Indiana Office of Technology for staff and offender use.

H. Technology Violations

All violations of this policy and administrative procedure shall be reported in writing to the Executive Director of Technology Services and the Information Security Officer.

XIV. APPLICABILITY:

This policy and administrative procedure is applicable to all Department facilities, staff, and offenders, except those offenders on Parole, and to those facilities that are operating under a court order or consent decree that mandates different procedures.

signature on file

Robert E. Carter, Jr.
Commissioner

Date