State of Indiana Indiana Department of Correction	Effective Date	Page 1 of	Number
	12/1/2020	7	04-05-104

POLICY AND ADMINISTRATIVE PROCEDURE
Manual of Policies and Procedures

Title
OFFENDER ACCESS TO INFORMATION TECHNOLOGY

Legal References (includes but is not limited to)	Related Policies/Procedures (includes but is not limited to)	Replaces: New
11-8-5-2	04-03-101 04-03-103 04-03-111	

I. PURPOSE:

The purpose of this policy and administrative procedure is to establish requirements for the access and use of information technology hardware and software by the offender population under the direct supervision of Indiana Department of Correction (IDOC) employees or other authorized individuals.

II. POLICY STATEMENT:

It is the policy of the Indiana Department of Correction that offender access to information technology (IT) Hardware and Software be limited to pro-social, treatment, educational, career technical, law library, and industrial program purposes under the direct supervision of staff or other authorized individuals. Offender access to IT Hardware, Software, and System Assets capable of accessing offender, employee, victim, security, operational, or any other sensitive or confidential IDOC information, data, or records is strictly prohibited. This policy and administrative procedure shall be reviewed annually and updated as necessary.

III. DEFINITIONS:

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

A. DIRECT SUPERVISION: The frequent, nonscheduled, direct, and unimpeded personal observation and contact between one (1) 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 policy and administrative

procedure, and this specific definition, the use of IDOC surveillance cameras does not constitute direct supervision.

B. 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, tape drives, servers, switches, routers, cable, fiber, etc.

C. IMAGING SOFTWARE: Specialized software used to copy an image of the entire and exact contents, which includes data and structure information, of a computing storage device, such as a server or hard drive on a PC.

D. LOCAL AREA NETWORK (LAN): A communication network that services several IT device users within a small or confined geographic area.

E. 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.

F. PORTABLE COMPUTING REMOVAL COMPONENTS: Detachable equipment items, supply items or other electronic objects used in conjunction with a portable computing device, such as cameras.

G. RECORD: Any item that is kept by the IDOC that: (1) is stored on a fixed medium, including an electronic or digital medium (2) is created, received, or sent under the jurisdiction of the IDOC and (3) documents the organization, functions, policies, decisions, procedures, operations, or other activities of the IDOC.

H. SENSITIVE DATA: Any type of data that presents a high or medium degree of risk if released or disclosed without authorization. There is a high degree of risk when unauthorized release or disclosure is contrary to a legally mandated confidentiality requirement. There may be a medium risk and potentially a high risk in cases for which an agency has discretion under the law to release data, particularly when the release must be made only according to agency policy or procedure. The data may be certain types of PII that is also sensitive, such as medical information, social security numbers, and financial account numbers. In addition, the data may be other types of information not associated with a particular individual such as security and infrastructure records, system administrative passwords, trade secrets and business bank account information.

I. 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.

J. STORAGE MEDIA: Mobile removable readable or write-able computing data storage objects, such as CDs, CD-R discs, DVD's, flash memory cards, USB jump drives and diskettes.

K. 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 Indiana Department of Correction and, therefore, must be protected by the appropriate security requirements to ensure business continuity.

L. VIDEO GAME CONSOLE: A specialized IT computing hardware device with the primary function of outputting a video signal to display video game content on a television or monitor. Components of a video game console include the hardware computing device, one or more handheld controllers, joysticks or pads, which connect to the hardware computing device, and game cartridges or cards that are inserted into the hardware computing device. Depending on its manufacturing date, a video game console may have wireless capability, portable computing media capability or the capability to stream a video signal between multiple game consoles. Video game console manufacturers include but are not limited to PlayStation, Wii, XBox, GamePop, GameStick and GameCube.

M. WIDE AREA NETWORK (WAN): A communication network that services multiple IT device users or interconnected IT systems within a large geographic area.

N. WIPING SOFTWARE: Software used to render all data on a hard drive unreadable and thus, inaccessible.

O. WIRELESS: A technology that uses various electromagnetic spectrum frequencies, such as radio and infrared, to communicate services, such as data and voice, without relying on hardwired connections, such as cable and fiber optics.

IV. PROCEDURES:

A. Offenders are strictly prohibited from:

1. Specifying, designing, purchasing, installing, operating, maintaining, or servicing any IT Hardware, Software, or System Assets that are used in the administrative operations of the IDOC (e.g., count sheets, pass lists, bed rosters, any confidential or sensitive data, any security related information, etc.).

2. Receiving or possessing any technical documentation, in any format, that describes the handling, functionality, and/or architecture of IT Hardware, Software, or System Assets pertaining to the administrative operations of the IDOC.

3. Receiving or possessing any technical documentation, in any format, that provides information or instructions on exploiting weaknesses in a computer system or network.

4. Receiving, possessing, or using any Hardware or Software NOT specifically designated for pro-social, treatment, educational, career technical, law library, or industrial program purposes approved by the managing officer.

5. Accessing any Hardware, Software, or System Assets that are part of a LAN or WAN system used in the administrative operations of the IDOC or to access the internet or IDOC intranet.

6. Assigning any passwords to any IDOC Hardware, Software, or files maintained on any LAN or WAN system.

7. Accessing any IDOC online data systems such as the offender management system.

8. Accessing any Software used in the administrative operations of the IDOC that resides on any Hardware.

9. Receiving, possessing, or accessing any Hardware, including Portable Computing Devices and their removal components, used to connect to any IDOC online data system or to other Software.

10. Receiving, possessing, or using any Storage Media, which is prohibited property, used in the administrative operations of the IDOC.

11. Receiving, possessing, or using any Storage Media, which is prohibited property, outside of the specific areas designated by the managing officer/designee.

12. Accessing any unauthorized wireless network used in the administrative operations of the IDOC or any wireless network used by individuals, organizations, or other entities outside the IDOC.

13. Using any personal Hardware or its associated Software, including Handheld Game Consoles, Video Game Consoles, or other electronic devices, to access, use, store, or transmit data, records, or other information that is used in the administrative operations of the IDOC or that could otherwise compromise, in any manner, anyone's safety and security.

14. Sharing any Hardware or Software passwords issued to them by their supervisor with others.

15. Accessing IT Hardware and Software for pro-social, treatment, educational, career technical, law library, and industrial program purposes without being under the direct supervision of staff or other authorized individuals.

16. Accessing, possessing, installing, or using any wiping software or any imaging software.

17. Installing, maintaining, supporting, or servicing any IDOC system assets, including system assets associated with the offender educational labs.

B. Offenders are permitted to:

1. Access and use standalone Hardware and Software to perform non-administrative functions (i.e., desktop publishing, simple word processing, data entry into databases and spreadsheets, etc.) under the direct supervision of staff or other authorized individuals and pursuant to the approval of the managing officer/designee.

2. Access and use the resources distributed by the educational labs or standalone Hardware and Software and access LAN and WAN systems NOT connected to IDOC's network, but otherwise specifically designated for pro-social, treatment, educational, career technical, law library or industrial program purposes under the direct supervision of staff or other authorized individuals and pursuant to the approval of the managing officer/designee.

3. Access and use Storage Media in the specific areas designated by the managing officer/designee. In said areas, the use of the Storage Media shall be strictly controlled by direct supervision of staff or other authorized individuals and the use shall be documented by the appropriate supervisor on the Sign-Out/Sign-In Log. The log shall be reviewed at regular intervals by the managing officer/designee.

4. Use passwords to access and use the aforementioned designated standalone Hardware and Software, LAN and WAN systems and storage media under the direct supervision of staff or other authorized individuals so long as the passwords are issued by the appropriate supervisor and are documented in a written log maintained by the appropriate supervisor. The written log shall be reviewed at regular intervals by the managing officer/designee.

5. Access inoperable IDOC System Assets that are being decommissioned, salvaged, repurposed, or physically moved from one location to another so long as the access is directly supervised by a staff member or other authorized individuals assigned by the managing officer/designee.

C. Process for Offender Technology Use Approval

All proposed requests for offender technology shall be reviewed by the Executive Director of Technology Services and Director of Offender Technology to ensure all offender accessible devices and/or systems are researched and approved as meeting any security protocols established by the IDOC Information Security Officer and the Indiana Office of Technology. Proposals for offender technology.

D. Donated and Repurposed System Assets

1. No IDOC facility or IDOC office shall accept, for offender use, any donated computing hardware, software, portable computing devices, portable computing removal components, storage media, wireless hardware, telecommunications equipment, electronics equipment ,or any other non-IDOC system asset from any individual or organization without the prior written approval of the Executive Director of Technology Services or designee.

2. No IDOC facility or IDOC office shall assign, reassign, or otherwise repurpose, for offender use, any new IDOC computing hardware, software, portable computing devices, portable computing removal components, storage media, wireless hardware, telecommunications equipment, electronics equipment, or any other IDOC system asset purchased or obtained for authorized users to perform their official duties.

3. No IDOC facility or IDOC office shall assign, reassign, or otherwise repurpose, for offender use, any IDOC computing hardware, software, portable computing devices, portable computing removal components, storage media, wireless hardware, telecommunications equipment, electronics equipment or any other IDOC system asset that is scheduled to be disposed of and/or salvaged.

E. Offender Technology Violations

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

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. Date

Commissioner