I. AUTHORITY

Ohio Revised Code 5120.01 authorizes the Director of the Department of Rehabilitation and Correction, as the executive head of the department, to direct the total operations and management of the department by establishing procedures as set forth in this policy.

II. 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 Ohio Department of Rehabilitation and Correction (ODRC).

III. APPLICABILITY

This policy applies to all Ohio Department of Rehabilitation and Correction (ODRC) employees and contractors.

IV. DEFINITIONS

**Authorized User** - An ODRC 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 and telecommunications technology 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 Ohio.

**Bulk Material** - Cables, wires, etc. that can be used to breach the security of the institution and shall, therefore, be controlled and secured. The Institution Specific Tool Control Information form (DRC2327) shall include language explaining how this shall be accomplished.

**Chief Information Security Officer (CISO)** - The technical staff member assigned to ODRC that, in collaboration with the Department of Administrative Services, Office of Information Technology, chief of BITS and other BITS technical staff members, is responsible for the security oversight of ODRC’s information technology system assets by establishing appropriate system asset security standards and risk controls to identify, develop, implement, maintain and support security processes across the ODRC information technology enterprise and to respond to system asset security incidents.
**Computer** - An electronic hardware device for storing and processing data, typically in binary form, according to instructions given to it in a variable program.

**Computer Room/Cage** - A secure location approved by the chief of security for storage of computers and hardware. This location shall have at minimum a single door and a high security lock. Inmates shall not be permitted to enter into the computer room/cage.

**Direct Supervision** - The frequent, nonscheduled, direct and unimpeded personal observation and contact between one or more ODRC staff members or other authorized individuals and inmates 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 this specific definition, the use of ODRC surveillance cameras does not constitute direct supervision.

**Hardware** - The tangible, material parts of any information technology device or system including desktop computers, laptops, tablet personal computers, monitors, keyboards, speakers, printers, central processing units (CPU), disk drives, tape drives, servers, switches, routers, cable, fiber, etc. ODRC information technology hardware is subject to the requirements contained in ODRC policy 22-BUS-08, Inventory Control of Property, Supplies and Other Assets.

**Information Technology (IT) Department** - The department charged with establishing, monitoring and maintaining information technology systems and services for ODRC – DYS shared services.

**Intermediate Distribution Frame (IDF)** - A wiring rack located between the MDF and the intended end user devices (telephones, routers, PCs, etc.).

**Main Distribution Frame (MDF)** - A cable rack that interconnects and manages the telecommunications wiring between itself and any number of IDFs.

**OAKS Asset Management System (OAKS AM)** - A software application that maintains detailed and categorized asset information, tracks asset activity, calculates depreciation and reports comprehensive asset information. It is supported by the Department of Administrative Services and made accessible to state agencies to use to meet their statutory inventory requirements.

**Portable Computing Device** - Any mobile electronic computer instrument or mechanism that allows a person to move from place to place and use or access information technology services, products and resources. Portable computing devices include air cards, laptops, tablet personal computers, smartphones and other similar handheld mobile electronic instruments or mechanisms.

**Portable Computing Media** - Any device that is capable of storing data and not necessarily required to be capable of processing data such as CD’s, CD-R discs, DVD’s, flash memory cards, USB jump drives and diskettes, magnetic tapes, solid state drives, external/removable hard drive, etc. Portable computing media devices known as “storage media”.

DRC 1362
Software - The intangible computer programs, procedures, algorithms, related data and associated documentation stored in an information technology device or system, 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, test ware, firmware, freeware, retail software, device drivers, programming tools and application software. ODRC information technology software is subject to the requirements contained in ODRC policy 22-BUS-08, Inventory Control of Property, Supplies and Other Assets.

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 ODRC or DAS OIT to authorized users and are necessary to conduct state government business and support the IT requirements of the ODRC and, therefore, must be protected by the appropriate security requirements to ensure business continuity.

Thin-Client - An end point computing device without an operating system that is purpose-built for remote access to a server.

V. POLICY

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

VI. 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 ODRC policy 05-OIT-10, 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.

3. Inmate access to information technology hardware, software and system assets capable of accessing inmate, employee, victim, security, operational or any other sensitive or confidential ODRC information, data or records is strictly prohibited, in accordance with ODRC policy 05-OIT-11, Inmate Access to Information Technology.
4. All inmate access to ODRC information technology hardware and software shall be limited to pro-social, treatment, educational, career technical, law library and industrial program purposes through ODRC 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 ODRC policy 05-OIT-21, Inventory, Donation, Transfer and Disposal of ODRC IT Hardware and Software.

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 CISO or designee.

7. In accordance with ODRC policy 22-BUS-08, Inventory Control of Property, Supplies, and Other Assets and ODRC policy 05-OIT-21, Inventory, Donation, Transfer and Disposal of ODRC IT Hardware and Software and in coordination with the Infrastructure Specialist and the business office, an updated and printed hardware and software inventory list shall be maintained. This list shall include all data contained in the OAKS Asset Management System.

8. Staff shall not move any stationary computer, hardware, portable computing media and/or computing devices without authorization from the institution infrastructure specialist and business office.

9. Any computer, hardware, software, portable computing media or portable computing devices possessed by inmates without the proper approval as defined in ODRC policy 05-OIT-11, Inmate Access to Information Technology, shall be confiscated as major contraband. The contraband shall be stored in a secured manner in such a way that access to the major contraband is limited to the institutional investigator, the Ohio State Highway Patrol (OSHP), or managing officer.

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

11. All information technology network hardware, to include MDF and IDF servers and switches, shall be maintained in a secured computer room/cage with access limited to ODRC information technology 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 pursuant to ODRC policy 22-BUS-08, Inventory Control of Property, Supplies, and Other Assets and ODRC policy 05-OIT-21, Inventory, Donation, Transfer and Disposal of ODRC IT Hardware and Software in order to ensure ready identification of the device and its location.
C. **Bulk Material**

All data cable, when not being utilized (i.e., bulk data cable), shall be controlled and secured by the information technologist, in accordance with ODRC policy 310-SEC-36, Tool Control, section VI.F.7. Bulk data cable in abundance, not for a project, shall be stored in a designated secure location without inmate access. At minimum, the material ends shall be marked or painted in a highly visible color, which easily identifies tampering. Institutions shall identify the color of paint on bulk material in the Institution Specific Tool Control Information form (DRC2327).

D. **Key Control**

Key access to all computer rooms/cages shall be restricted to ODRC – DYS shared services information technology staff members, chief of security/designee.

E. **Computer Inspection**

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

   1. Search for stored and/or written down user names and passwords;
   2. Staff members leaving unlocked computers accessible to inmates;
   3. Conducting a visual inspection of the work area for unauthorized hardware;
   4. 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 sent to the managing officer/designee for review and, upon completion of the review, shall be submitted to the CISO/designee. The appropriate facility information technology staff member shall maintain the completed summary report on file for review by the respective regional operations manager.

F. **Computer Storage**

1. All computer hardware, when not in use, shall be stored in the secure computer room/cage designated by the chief of security.

2. Inventory control procedures shall include the use of a Perpetual Inventory Log (DRC2671) for desktop computers, laptops, tablet personal computers, central processing units (CPU), servers, switches, routers while secured in the computer room/cage.
3. The chief of security shall assign a security staff member to conduct a quarterly inventory of the computer room/cage. The report shall be forwarded to the chief of security for review.

G. 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 and shall be subject to the asset management requirements of ODRC policy 22-BUS-08, Inventory Control of Property, Supplies, and Other Assets and ODRC policy 05-OIT-21, Inventory, Donation, Transfer and Disposal of DRC IT Hardware and Software. 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. Inmates shall not be allowed access to inoperable ODRC 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 (i.e., 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 and accounted for pursuant to the inventory procedures in place in the computer room/cage.

H. Inventory

1. Computers and hardware shall be affixed with at least one asset identification tag within fifteen (15) business days from the date received by the institution and uploaded in OAKS AM within thirty (30) business days from the date received.

2. The asset processor/designee assigned to each location within ODRC shall be responsible for directing and conducting an annual physical inventory of all computers and hardware recorded in the OAKS AM each fiscal year.

I. USB Drives

1. The managing officer and/or designee will maintain a list of USB drives and other portable computing media approved by the ODRC – DYS Shared Services chief of the Bureau of Information Technology or designee. A copy of the updated list shall be provided to all entry points of the institution and available to the officer on post for review. The assigned officer shall ensure no USB drives enter the facility without being on the approved list.

2. When not in use, all approved USB drives shall be secured in a locked cabinet/drawer with the Registration for Electronic Device form (DRC1818).
J. Technology Violations

All violations of this policy shall be reported pursuant to the requirements of ODRC policy 01-COM-08, Incident Reporting and Notification.

Related Department Forms:

- Incident Report: DRC1000
- Registration for Electronic Devices: DRC1818
- Institution Specific Tool Control Information form: DRC2327
- Perpetual Inventory Log: DRC2671