



SUBJECT: Inventory, Donation, Transfer & Disposal of DRC IT Hardware & Software	PAGE <u> 1 </u> OF <u> 11 </u>
	NUMBER: 05-OIT-21
RULE/CODE REFERENCE: 5120.01, 5120.22; DAS OIT policy ITP-E.1	SUPERSEDES: 05-OIT-21 dated 02/02/15
RELATED ACA STANDARDS:	EFFECTIVE DATE: December 19, 2016
	APPROVED: 

I. AUTHORITY

This policy is issued in compliance with Ohio Revised Code 5120.01 which delegates to the Director of the Department of Rehabilitation and Correction the authority to manage and direct the total operations of the Department and to establish such rules and regulations as the Director prescribes.

II. PURPOSE

The purpose of this policy is to establish requirements for the inventory, transfer and disposal of Ohio Department of Rehabilitation and Correction (DRC) system assets pursuant to the requirements of Department of Administrative Services, Office of Information Technology (DAS OIT) Policy ITP-E.1, entitled, Disposal, Servicing and Transfer of IT Equipment.

III. APPLICABILITY

This policy applies to all Ohio Department of Rehabilitation and Correction (DRC) authorized users who are issued DRC system assets, including leased or rented hardware or software.

IV. DEFINITIONS

Authorized User - A DRC employee, contractor, intern, volunteer or other agent of the State who is authorized at a technical level to administer and support/maintain state computing information technology systems and telecommunications technology systems or is authorized at an end user level, to have access to and use state computing information technology systems and telecommunications technology systems for business purposes on behalf of the State of Ohio.

Confidentiality - The assurance that information is disclosed only to those systems or persons who are intended to receive it. Information systems that must ensure confidentiality will likely deploy techniques such as passwords and encryption to secure data. Information that may require confidentiality include, but are not limited to, nonpublic customer information, healthcare records, information about a pending criminal case or administrative investigation, infrastructure specifications and administrative passwords.

Confidential Personal Information (CPI) - Personal information that falls within the scope of section 1347.15 of the Ohio Revised Code and that DRC is prohibited from releasing under Ohio's public records law.

Data - The coded representation of quantities, objects and actions. Data is often used interchangeably with the common term, "information."

Data Owners - DRC managing directors/designees that are authorized users responsible for identifying and classifying data for their respective areas.

Demagnetize - To reduce the magnetic flux to virtual zero by applying a reverse magnetizing field, which, when properly completed, renders any previously stored data on magnetic media unreadable. This procedure is also referred to as "degaussing."

Destroy - To render system assets unusable and the data contained within the system asset unrecoverable. Destroying includes, but is not necessarily limited to, shredding, incineration and drilling holes.

Disposal - The final transfer of ownership or custody of information technology hardware, typically when the hardware has reached its end-of-life and requires replacement.

Donation - Transferring ownership and custody of a system asset to another entity.

Hardware - The tangible, material parts of any information technology 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. DRC information technology hardware is subject to the requirements contained in DRC policy 22-BUS-08, Inventory Control of Property, Supplies and Other Assets.

Intellectual Property - A commercially valuable product of the human intellect in a concrete or abstract form, such as copyrightable work, a protectable trademark, a patentable invention or a trade secret.

License - A contract that authorizes access to software and data and outlines rights regarding the use, distribution, performance, modification or reproduction of software and data.

Licensed Software - Software in any form, whether commercial, propriety or gratuitous, that is provided by the intellectual property holder under terms of a contract that governs use, copying, modification and distribution.

Overwrite - To write patterns of new data on top of the data already stored on a magnetic medium.

Personally Identifiable Information (PII) - Information that can be used directly or in combination with other information to identify a particular individual. PII includes:

- A name, identifying number, symbol or other identifier assigned to a person.
- Any information that describes anything about a person.
- Any information that indicates actions done by or to a person.
- Any information that indicates that a person possesses certain personal characteristics.

Risk Assessment - A process performed to analyze the threats to and the vulnerabilities of DRC system assets to determine the potential impact that loss of data, capability or functionality would have on the business operation of an organization. Risk assessment of system assets provides a foundation for information technology risk management and the attainment of optimal levels of information technology functionality and security at both the desktop and enterprise levels and shall be completed pursuant to DAS OIT Standard ITS-SEC-02, entitled, Enterprise Security Controls Framework.

Sanitize - To expunge data from system assets so that data recovery is reasonably prohibitive. Sanitizing includes, but is not necessarily limited to, overwriting, demagnetizing, and destroying.

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 personally identifiable information (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.

Software - The intangible computer programs, procedures, algorithms, related data and associated documentation stored in an information technology 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. Software can be licensed or unlicensed but, in any event, software used for official DRC business is subject to the requirements contained in DRC policy 22-BUS-08, Inventory Control of Property, Supplies and Other Assets.

System Asset - Computer hardware, software, networks, data and/or services or resources that are necessary to support the information technology requirements of the DRC and therefore, must be protected by the appropriate security requirements to ensure business continuity.

V. POLICY

It is the policy of the Ohio Department of Rehabilitation and Correction (DRC) to maintain an accurate inventory of all DRC system assets pursuant to all applicable DRC requirements and to process the donation, transfer, and disposal of DRC system assets pursuant to the requirements of Department of Administrative Services, Office of Information Technology Policy ITP-E.1, entitled, Disposal, Servicing and Transfer of IT Equipment.

VI. PROCEDURES

A. Inventory of DRC Information Technology Hardware and Software

1. Upon receipt of any information technology hardware, including leased or rented hardware, or software acquisition at a DRC worksite, the manager or designee at the worksite responsible for receiving the delivery shall physically count the hardware or software. Discrepancies between the shipping invoice and the physical count shall be noted and reported immediately to the appropriate staff member in the worksite business office.
2. Upon completion of the physical count, the manager or designee shall advise the worksite's designated asset processor or designee of receipt of the hardware or software acquisition.
 - a. Pursuant to DRC policy 22-BUS-08, Inventory Control of Property, Supplies and Other Assets, the asset processor or designee shall ensure each piece of hardware or software is affixed with a unique identifying bar code inventory label or electronic medium device or otherwise assigned a unique identifying bar code inventory label, and that all hardware or software is entered into the OAKS Asset Management System within the appropriate time period.
 - b. The asset processor or designee shall advise the appropriate information technology employee at the worksite of the hardware or software acquisition. Receipt of hardware or software acquired for the Operation Support Center (OSC) shall be reported to the chief of the Bureau of Information Technology Services (BITS) or designee.
3. Information technology hardware and packaged, licensed software shall be stored in the worksite storeroom, warehouse or other secured storage area. A perpetual inventory shall be maintained for the hardware and software and a physical inventory of the hardware and software shall be conducted pursuant to the timeframes and manner prescribed by DRC policy.
4. The designated worksite agency asset processor shall update information technology hardware and software inventory information in the OAKS Asset Management System when appropriate and especially when the hardware or software is donated, transferred or disposed of when it reaches the end of its functional DRC lifecycle.
5. The designated worksite agency asset processor shall ensure all information technology hardware and software at the worksite is included in the physical inventory conducted at

least once per biennium pursuant to DRC policy 22-BUS-08, Inventory Control of Property, Supplies and Other Assets.

6. The chief of BITS shall designate a BITS staff member to serve as the BITS agency asset processor or designee. They shall be responsible for performing all the inventory duties for the software and software licensing assigned to or maintained by BITS, including programming software, system software, operating system software, testware, firmware, freeware, retail software, device drivers, programming tools, and application software.

B. Donation of DRC Information Technology Hardware and Software to Non-DRC Individuals or Organizations

1. Authorized users do not have authority to unilaterally donate any DRC system asset to non-DRC individuals or organizations.
2. The following process shall be followed when a request is made to donate any DRC information technology hardware, excluding leased or rented hardware, or software to a non-DRC individual or organization:
 - a. Requests from non-DRC individuals or organizations to donate DRC information technology hardware or software shall be referred to the appropriate managing director for review and assessment.
 - b. If the managing director or designee determines the donation request has merit, the managing director/designee shall formally notify and provide the chief of BITS with all available information about the request, such as the requestor's contact information, a list of the requested hardware or software, the rationale for the request and the timeframes to fulfill the request.
 - c. The chief of BITS shall assign a DRC authorized user at the technical level the task of conducting a risk assessment of the requested hardware or software.
 - d. The authorized user at the technical level shall conduct the risk assessment, taking special care to identify any PII, CPI or sensitive data that resides on the hardware or software and, within five (5) business days of completing the risk assessment, shall complete a written report, which may be in an e-mail format, that contains the risk assessment findings and results. The report shall be submitted to the chief of BITS and a copy shall be submitted to the appropriate managing director/designee.
 - e. The chief of BITS shall review the report and determine whether the donation request will be granted and, if granted, approve the appropriate course of action that must be taken to sanitize the hardware or software. Overwriting shall be the preferred method for sanitizing. The chief of BITS shall advise the appropriate managing director/designee and authorized user at the technical level of the donation decision and the course of action that must be taken to sanitize the hardware or software prior to the physical transfer. As part of the sanitizing process, all PII, CPI and sensitive data shall, at a minimum, be overwritten on the hardware or software. More rigorous

sanitizing methods, such as demagnetizing, increasing the number of overwrites or physical destruction, shall be utilized as the level of data confidentiality and risk increase.

- f. Once the donation has been approved and the hardware or software has been sanitized pursuant to the direction of the chief of BITS, the managing director/designee shall instruct the worksite's agency asset processor or designee to take the necessary action to comply with state salvage requirements and, upon approval from DAS State Salvage, remove the requested hardware or software from the worksite's inventory in the OAKS Asset Management System. The worksite's agency asset processor or designee shall then proceed with the physical donation of the requested hardware or software to the non-DRC individual or organization.
- g. The appropriate authorized user at the technical level shall document the donation in the DRC IT Donation, Maintenance/Repair and Disposal Form (DRC1636).

C. Transfer of DRC Information Technology Hardware or Software to an Approved Vendor for Maintenance and Repair

1. The following process shall be followed when the decision has been made to transfer DRC hardware, excluding leased or rented hardware, or licensed or unlicensed software to an approved vendor for maintenance and repair:
 - a. The appropriate authorized user at the technical level shall conduct a risk assessment of the hardware or software taking special care to identify any PII, CPI or sensitive data that resides on the hardware or software.
 - b. In addition to conducting the risk assessment, the authorized user at the technical level shall identify the specific maintenance/repair necessary for the hardware or software, ensure a current, written signed IT Vendor Confidentiality Agreement (DRC3389) exists, make the appropriate contacts with the vendor to initiate the maintenance/repair process and complete any DRC or vendor maintenance and repair request reports or documents.
 - c. After completing the risk assessment, the information technology employee shall take the action identified during the risk assessment to sanitize the hardware or software. As part of the sanitizing process, all PII, CPI and sensitive data shall, at a minimum, be overwritten on the hardware or software. More rigorous sanitizing methods, such as demagnetizing, increasing the number of overwrites or physical destruction, shall be utilized as the level of data confidentiality and risk increase.
 - d. After the hardware or software is sanitized, the authorized user at the technical level shall provide the hardware or software to the vendor for completion of the required maintenance/repair.
 - e. When the maintenance/repair has been completed and the hardware or software is returned to the worksite, the authorized user at the technical level shall reconfigure the hardware or software and reissue it to the appropriate staff member or return it to storage.

- f. The authorized user at the technical level shall document the maintenance and repair in the DRC IT Donation, Maintenance/Repair and Disposal Form (DRC1636)
2. The following process shall be followed when the decision has been made to transfer DRC leased or rented information technology hardware to an approved vendor for maintenance and repair:
 - a. The appropriate authorized user at the technical level shall conduct a risk assessment of the hardware taking special care to identify any PII, CPI or sensitive data that resides on the hardware.
 - b. In addition to conducting the risk assessment, the authorized user at the technical level shall identify the specific maintenance/repair necessary for the hardware, as specified by the hardware vendor, ensure a current, written signed IT Vendor Confidentiality Agreement (DRC3389) exists, make the appropriate contacts with the vendor to initiate the maintenance/repair process, request that overwriting be completed to sanitize the hardware, and complete any DRC or vendor maintenance and repair request reports or documents.
 - c. After completing the risk assessment, the authorized user at the technical level shall consult with the vendor and take the appropriate action to sanitize the hardware. As part of the sanitizing process, all PII, CPI and sensitive data shall be, at a minimum, overwritten on the hardware. More rigorous sanitizing methods, such as demagnetizing, increasing the number of overwrites or physical destruction, shall be utilized as the level of data confidentiality and risk increase.
 - d. After the hardware is sanitized, the authorized user at the technical level shall provide the hardware to the vendor for the maintenance/repair.
 - e. When the maintenance/repair has been completed and the hardware returned to the worksite, the authorized user at the technical level shall reconfigure the hardware and reissue it to the appropriate staff member or return it to storage.
 - f. The authorized user at the technical level shall document the hardware maintenance and repair in the DRC IT Donation, Maintenance/Repair and Disposal Form (DRC1636).

D. Disposal of DRC Information Technology Hardware or Software

1. The following process shall be followed when DRC information technology hardware, excluding leased or rented hardware or software is at the end of its functional lifecycle and the decision has been made to dispose of the hardware or software.
 - a. The appropriate authorized user at the technical level shall conduct a risk assessment of the hardware or software taking special care to identify any PII, CPI or sensitive data that resides on the hardware.
 - b. After completing the risk assessment, the authorized user at the technical level shall take the action identified during the risk assessment to sanitize the hardware or software. As part of the sanitizing process, all PII, CPI and sensitive data shall, at a

minimum, be overwritten on the hardware or software. More rigorous sanitizing methods, such as demagnetizing, increasing the number of overwrites or physical destruction, shall be utilized as the level of data confidentiality and risk increase.

- c. When the hardware or software has been sanitized, the authorized user at the technical level shall contact the worksite asset processor or designee, who shall take the necessary steps to remove the hardware or software from the OAKS Asset Management System and, if appropriate, process the hardware or software as state salvage, pursuant to all applicable DRC and DAS State Salvage rules and regulations.
 - d. The authorized user at the technical level shall document the disposal in the DRC IT Donation, Maintenance/Repair and Disposal Form (DRC1636).
2. The following process shall be followed when a decision is made to contract with a vendor to dispose of DRC information technology hardware, excluding leased or rented hardware, or software that is at the end of its functional lifecycle:
- a. The authorized user at the technical level shall ensure that a current, written signed IT Vendor Confidentiality Agreement (DRC3389) exists.
 - b. The appropriate authorized user at the technical level shall advise the chief of BITS/designee of the decision to contract with a vendor and shall, if requested, provide the chief of BITS/designee with the vendor's written, signed statement.
 - c. The authorized user at the technical level shall conduct a risk assessment of the hardware or software taking special care to identify any PII, CPI or sensitive data that resides on the hardware.
 - d. The authorized user at the technical level shall contact the worksite agency asset processor or designee who shall take the necessary steps to remove the hardware or software from the OAKS Asset Management System.
 - e. The authorized user at the technical level shall, at a minimum, overwrite all PII, CPI and sensitive data on the hardware or software. More rigorous sanitizing methods, such as demagnetizing, increasing the number of overwrites or physical destruction, shall be utilized as the level of data confidentiality and risk increase. The authorized user at the technical level shall also contact the vendor to make the necessary arrangements to provide the hardware or software to the vendor.
 - f. The authorized user at the technical level shall document the disposal on the DRC IT Donation, Maintenance/Repair and Disposal Form (DRC1636).
3. The following process shall be followed when leased or rented DRC information technology hardware is at the end of its functional lifecycle and the decision has been made to dispose of the hardware:
- a. The appropriate authorized user at the technical level shall conduct a risk assessment of the hardware taking special care to identify any PII, CPI or sensitive data that resides on the hardware.

- b. After completing the risk assessment, the authorized user at the technical level shall consult with the vendor, identify the appropriate procedure for sanitizing the hardware and take the action identified during the risk assessment and vendor consultation to sanitize the hardware. As part of the sanitizing process, all PII, CPI and sensitive data shall be, at a minimum, overwritten on the hardware. more rigorous sanitizing methods, such as demagnetizing, increasing the number of overwrites or physical destruction, shall be utilized as the level of data confidentiality and risk increase
- c. When the hardware has been sanitized, the authorized user at the technical level shall contact the worksite agency asset processor or designee, who shall take the necessary steps to remove the hardware from the OAKS Asset Management System.
- d. Upon removal of the hardware from the OAKS Asset Management System, the authorized user at the technical level shall provide the hardware to the vendor.
- e. The authorized user at the technical level shall document the disposal in the DRC IT Donation, Maintenance/Repair and Disposal Form (DRC1636).

E. DRC Risk Assessment

1. A DRC risk assessment of DRC information technology or software shall be performed only by an authorized user at the technical level approved by the chief of BITS.
2. At a minimum, a DRC risk assessment of DRC information technology hardware, including leased or rented hardware, or software completed pursuant to this policy, must include the following steps:
 - a. Verification of the inventory status of the hardware or software via a search of the OAKS Asset Management System.
 - b. Identification of the type of data that resides on the hardware or software, the data owners and whether any or all of the data is PII, CPI or sensitive data.
 - c. Identification of any active intellectual property licenses residing on or associated with the hardware or software.
 - d. Identification of the most appropriate course of action to sanitize the hardware or software.
 - e. Verification, when appropriate, that a current, written, signed IT Vendor Confidentiality Agreement (DRC3389) exists.
3. The DRC authorized user at the technical level performing the risk assessment must consult with the chief of BITS/designee when there are questions or concerns about the most appropriate course of action to properly sanitize any system asset.

F. Maintaining DRC IT Donation, Maintenance/Repair and Disposal Forms (DRC1636)

At the end of each quarter of the fiscal year, the DRC IT Donation, Maintenance/Repair and Disposal Forms (DRC1636) completed during the quarter shall be provided to the worksite agency asset processor or designee who, in turn, shall maintain the form with other OAKS Asset Management System inventory documentation.

G. Requirements For a Current, Written Signed IT Vendor Confidentiality Agreement (DRC3389)

1. A current, written signed IT Vendor Confidentiality Agreement (DRC3389) shall be required from any vendor providing system asset maintenance and repair services to DRC. At a minimum, the vendor shall agree to:
 - a. Maintain the confidentiality of State data.
 - b. Access data only if it is necessary for maintenance or repair service purposes.
 - c. Destroy, sanitize or return the system assets pursuant to the requirements of DRC.
2. A current, written signed confidentiality agreement shall be required from any vendor providing system asset sanitizing services to DRC. At a minimum, the vendor shall agree to:
 - a. Maintain the confidentiality of state data.
 - b. Access data only if it necessary for sanitization purposes.
 - c. Sanitize the system assets pursuant to the requirements of DRC.

H. Prevention of Software Licensing Agreement Violations

1. Prior to donating or transferring any system asset, authorized users at the technical level shall perform the appropriate sanitizing procedures to reasonably prevent the violation of software licensing agreements, in accordance with DAS OIT Policy ITP-A.26, entitled, Software Licensing.

I. Disposal of System Assets Containing Universal Waste Batteries

1. System assets that contain universal waste batteries shall be disposed of in accordance with the requirements of Chapter 3745-273 of the Ohio Administrative Code.
 - a. Any universal waste battery that shows evidence of leakage, spillage, or damage that could cause leakage under reasonably foreseeable conditions shall be placed in a container prior to disposal. The container must be closed, structurally sound, compatible with the contents of the battery, and must lack evidence of leakage, spillage, or damage that could cause leakage under reasonably foreseeable conditions. The container must be clearly and legibly labeled or marked as “Universal Waste - Battery(ies),” “Waste Battery(ies)” or “Used Battery(ies)” in order to identify the contents as universal waste.
 - b. Any universal waste battery that does not show evidence of leakage, spillage or damage and, therefore, does not require disposal in a container must be clearly and legibly labeled or marked at time of disposal as “Universal Waste - Battery(ies),” “Waste Battery(ies)” or “Used Battery(ies).”

- c. DRC managing officers shall ensure refuse companies responsible for the pick-up, hauling and disposal of trash at DRC facilities and offices adhere to the above universal waste battery disposal requirements.

Related Department Forms:

DRC IT Donation, Maintenance/Repair and Disposal Forms	DRC1636
Information Technology Vendor Confidentiality Agreement	DRC3389