

SUBJECT: Portable Computing Devices, Media and Removable Components	PAGE <u> 1 </u> OF <u> 9 </u>
	NUMBER: 05-OIT-15
RULE/CODE REFERENCE: DAS OIT policy IT-14	SUPERSEDES: 05-OIT-15 dated 01/06/14
RELATED ACA STANDARDS:	EFFECTIVE DATE: October 28, 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, pursuant to the Ohio Department of Administrative Services, Office of Information Technology (DAS OIT) Policy IT-14, Data Encryption and Security Sensitive Data, for the use, security, management and control of state-owned portable computing devices, state-owned portable computing media and state-owned portable computing removable components assigned to Ohio Department of Rehabilitation and Correction (DRC) authorized users.

III. APPLICABILITY

This policy applies to all Ohio Department of Rehabilitation and Correction (DRC) authorized users assigned state-owned portable computing devices, portable computing media and portable computing removable components by DRC to conduct state business.

IV. DEFINITIONS

Administrator Privileges - Ability to modify computer system settings including access permissions associated with computer resources and data.

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 and to use state computing information technology systems and telecommunications technology systems for business purposes on behalf of the State of Ohio.

Basic Information Technology (IT) Security Awareness Training - IT security awareness training that provides DRC employees and other individuals that have access to DRC IT system assets with a basic understanding of the need for information security and the actions that individuals can take to maintain security and respond to suspected security incidents. An online training program, such as SANS Securing the Human, is a preferable training solution because it is standardized, readily available and generates appropriate training documentation.

Chief Information Security Officer (CISO) - The technical staff member assigned to DRC 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 DRC'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 DRC information technology enterprise and to respond to system asset security incidents.

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

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

Data Synchronization - The practice of updating data on two (2) systems so that the data that sets on the two (2) systems are identical.

Encryption - The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

Firewall - Either software or a combination of hardware and software that implements security policy governing data traffic between two (2) or more network segments or processes. Firewalls are used to protect internal networks, servers and workstations from unauthorized users or processes.

Identification and Authentication (I&A) - The verification of the identity of a requesting entity (a person, computer, system or process). Once it is determined who may have access to a system, the identification and authentication (I&A) process helps to enforce access control to the system by verifying system user identity. Computer systems may use a variety of techniques or combinations of techniques such as user-ID, password, personal identification number, digital certificates, security tokens or biometrics to enforce I&A, depending upon the level of access control required to protect the system.

Information Technology (IT) Security Incident - A violation or imminent threat of violation of information system/computer security policies, acceptable use policies, or standard security practices that threatens the confidentiality, integrity or availability of any system asset. Computer security incidents include, but are not limited to:

- Unauthorized access to any system asset;
- Denial of service for any system asset;
- Installation of malicious code on any system asset;
- Improper usage or access of any system asset;
- Scans, probes and attempted access of any system asset;
- Information spillage for any system asset;
- Loss or theft of a DRC computing device or DRC media;
- The compromise, in any way, of any confidential, non-public and or Personally Identifiable Information (PII).

Non-DRC Entity - An organization external to DRC or one or more individuals representing an organization external to DRC that are not authorized DRC users who request DRC sensitive data.

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.

Portable Computing Device - Any mobile electronic computer 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 Removable Components - Detachable equipment items, supply items or other electronic objects used in conjunction with a portable computing device, such as cameras.

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

Screen Locking - A mechanism to hide data on a visual display while the computer continues to operate. A screen lock requires authentication to access the data. Screen locks can be activated manually or in response to policies implemented by computer system administrators.

Screen Timeout - A mechanism to turn off a device or end a session when the electronic computing device has not been used for a specified time period.

Security Token - A portable, physical device that enables pre-approved access to information technology devices, data or systems.

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.

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.

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.

V. **POLICY**

It is the policy of the Ohio Department of Rehabilitation and Correction (DRC) to protect state-owned portable computing devices, portable computing media and portable computing removable components assigned to authorized users in compliance with DAS OIT policy IT-14, Data Encryption and Security Sensitive Data.

VI. **PROCEDURES**

A. **Physical Security**

1. Authorized users are assigned state-owned portable computing devices, portable computing media and portable computing removable components for the sole purpose of conducting state business and shall, therefore, take the following actions to protect these state-owned information technology items from unauthorized access and use.
 - a. When not in use, state-owned portable computing devices, portable computing media and portable removable computing components shall be stored in a secure environment, preferably in a locked office, locked drawer or locked cabinet.
 - b. When in use, state-owned portable computing devices, portable computing media and portable removable computing components shall not be left unattended for any period of time.
 - c. When an authorized user is traveling, state-owned portable computing devices, portable computing media and portable removable computing components shall remain under the authorized user's direct control. If direct control cannot be

maintained, then the authorized user shall take the necessary steps to temporarily store the state-owned devices, media or removable components in a secure manner.

- d. During business hours, state-owned portable computing devices, portable computing media and portable removable computing components may be stored temporarily in the locked trunk of a state or personal vehicle. However, during non-business hours, state-owned devices, media and removable components shall not be stored in any vehicle.
 - e. Authorized users shall not give any of their user names or passwords to unauthorized individuals nor permit unauthorized individuals to use or otherwise have access to their assigned portable devices, portable media or portable removable components.
 - f. DRC supervisors shall take the appropriate actions to retrieve and secure state-owned portable computing devices, portable computing media and portable computing removal components when an authorized user's period of employment, contract service, volunteer service or intern service terminates or when the authorized user's assignment no longer requires possession of a portable device, media or removal components. When portable devices, media or removal components are removed from service by a DRC supervisor, the supervisor will notify the appropriate worksite authorized user at the technical level who shall take control of the items and assess the items for reissue at the worksite.
 - g. State-owned portable computing devices, portable computing media and portable computing removable components shall be inventoried, removed from service, transferred and sanitized and disposed of pursuant to DRC policy 05-OIT-21, Inventory, Donation, Transfer and Disposal of DRC IT Hardware and Software. Pursuant to the aforementioned policy, special care shall be taken by the authorized user at the technical level when completing the required risk assessment, to identify any sensitive data or CPI that resides on a state-owned portable computing device or state-owned portable computing media and sanitize the device or media accordingly.
 - h. When storage of multiple state-owned portable computing devices, state-owned portable computing media and state-owned portable computing removable components is required at any DRC facility or office, the devices, media and components shall be stored in secure locations. Only authorized individuals shall be approved for access to the secure locations and the state-owned devices, media and components contained within the locations. Only authorized users at the technical level shall be approved to remove said devices, media and components from the secure locations.
2. Unless approved in writing by the DRC Chief of BITS, authorized users shall not connect non-state portable computing devices, portable computing media and portable computing removal components to state IT computing devices or systems. Further, DRC shall not assume responsibility or liability for the loss or corruption of non-state data, applications or software connected to state-owned IT computing devices or data systems.

3. Offender access to DRC portable computing devices, portable computing media and portable computing removal components shall be guided by DRC policy 05-OIT-11, Inmate Access to Computers.
4. The loss or theft of a state-owned portable computing device, portable computing media or portable computing removal component shall be reported by the authorized user to the user's supervisor pursuant to DRC policy 01-COM-08, Incident Reporting and Notification. In addition, if there is any suspicion that the state-owned portable computing device was stolen, the authorized user shall immediately report the suspected theft to the Ohio State Highway Patrol and, if deemed necessary by the user's supervisor, to local law enforcement. If the portable device, media or removal component contains sensitive data, including PII, or CPI or the portable device is connected to any online state data system, the authorized user shall report loss or theft immediately to the user's supervisor who, in turn, shall report the loss or theft to the chief of BITS.

B. System Security, Operation and Maintenance

1. The chief of BITS, in consultation with the CISO, shall establish and implement IT procedures, controls and user restrictions to ensure system security and the efficient operation and maintenance of state-owned portable computing devices, state-owned portable computing media and state-owned portable computing removal components. At a minimum, the chief of BITS shall ensure that security procedures and user restrictions across all DRC enterprise domains address the following requirements pursuant to the mandates promulgated by DAS OIT:
 - a. DRC sensitive data and CPI shall be accessed and secured on state-owned portable computing devices and state-owned portable computing media pursuant to the following requirements:
 - i. Using the data maintenance guidelines generated by the CISO during annual compliance reviews, completed pursuant to DRC Policy 05-OIT-23, DRC Data Identification and Classification Requirements, data owners shall identify, in writing, individual authorized users or specific groups of authorized users (e.g., parole officers, case managers, healthcare providers, etc.) in their respective areas that are approved to have access to DRC sensitive data and CPI on state-owned portable computing devices and state-owned portable computing media. At a minimum, the written authorization shall contain the sensitive data and CPI that may be accessed, stored and transmitted by the authorized user(s) and the business justification for the access, storage and transmission. Data owners shall provide the written authorization to the appropriate authorized users at the technical level in BITS and in DRC facilities who assign and service the state-owned devices and media and shall maintain the written authorization, which may be reviewed by the CISO on an annual basis during the aforementioned annual compliance reviews.
 - ii. All state-owned portable computing devices and state-owned portable computing media that access, contain and/or transmit sensitive data and CPI shall be secured by strong passwords and encryption, which may be employed at the data level, file level or operating system level.

- iii. In no event shall state-owned portable computing devices and state-owned portable computing media containing unencrypted sensitive data or CPI be stored or transported in a manner that is not physically secure to include the use of multiple layers of physical security.
- iv. Authorized users shall not use a state-owned portable computing device to transmit sensitive data or CPI through an unknown or untrusted channel or to an unknown or untrusted site.
- v. When an authorized user assigned a state-owned portable computing device is performing job duties in an approved alternate workplace, pursuant to DRC policy 35-PAY-09, Telecommunicating Procedures, DRC sensitive data and CPI shall be accessed and transmitted only through the authorized user's virtual privacy network (VPN) account.
- vi. All of the following requirements must be met for an authorized user to access, store, transmit or transport DRC sensitive data or CPI on a personal portable computing device or personal portable computing media:
 - a) An emergency must exist wherein a DRC device or media is not otherwise available to be assigned to the authorized user.
 - b) The access, storage, transmission or transport of the sensitive data or CPI and use of the personal device or personal media has been approved in writing by the appropriate data owner.
 - c) The personal device or personal media has been approved in writing by the chief of BITS or CISO.
- b. State-owned portable computing devices shall be configured with appropriate anti-virus software and the appropriate mobile security tracking software pursuant to requirements promulgated by the CISO.
- c. State-owned portable computing device operating systems shall be maintained with appropriate vendor security patches and updates by authorized DRC IT staff.
- d. State-owned portable computing devices shall not be equipped with remote system or application administrator privileges unless authorized by the chief of BITS. State-owned portable devices equipped with remote system administrator capabilities shall be assigned higher levels of security access in accordance with the increased risk of an IT cybersecurity breach or loss/theft of the device.
- e. Mandatory DRC system configurations, settings and software for state-owned portable computing devices shall not be modified without the prior authorization of the chief of BITS or CISO.

- f. State data, applications and other state system resources stored on state-owned portable computing devices shall be secured via the appropriate security framework pursuant to the requirements established by the CIO, which may include, but are not necessarily limited to:
 - i. Personal firewalls;
 - ii. BIOS passwords;
 - iii. Data / application encryption;
 - iv. Screen locking;
 - v. Screen timeout;
 - vi. Security tokens;
 - vii. Two-factor authentication;
 - viii. Virtual privacy network access;
 - ix. Disabling network access after a predetermined period of non-connection; and
 - x. Proxy settings that limit Internet access to work-related sites
 - g. DRC systems shall be configured with security update policies that restrict the use of portable computing media to encrypted drives.
 - h. The transmission of any state data over the DRC network via infrared, Bluetooth or other wireless technologies shall be secured pursuant to the requirements established by the CISO.
 - i. DRC regular system and data back-ups shall be performed at required intervals based on DRC's assessment of the confidentiality and criticality of the data maintained on each portable computing device as determined by the procedures mandated in DRC policy 05-OIT-23, DRC Data Identification and Classification Requirements. Back-ups shall be safeguarded and retained for the required period of time, commensurate with the data maintenance guidelines required in DRC policy 05-OIT-23, DRC Data Identification and Classification Requirements.
 - j. State-owned portable computing devices shall accommodate identification and authentication (I&A) password and PIN controls.
 - k. State-owned portable computing devices connected to the Internet shall comply with all requirements contained in DRC policy 05-OIT-10, Internet, Electronic Mail, and Online Services Use.
 - l. The sanitizing procedures mandated in DRC policy 05-OIT-21, Inventory, Donation, Transfer and Disposal of DRC IT Hardware and Software, shall be completed prior to the donation, transfer or disposal of any state-owned portable computing device or state-owned portable computing media.
2. When the chief of BITS or CISO is informed that a DRC IT security incident involving a state-owned portable computing device or state-owned portable computing media has occurred, or is threatened, the chief of BITS or CISO shall respond pursuant to the requirements of DRC policy 04-OIT-14, Information Technology Security Incident Response.

C. Security Awareness Training Requirement

1. Before an authorized user is assigned a state-owned portable computing device, the authorized user shall successfully completed Basic IT Security Awareness Training and the successful completion of the training shall be verified, pursuant to DRC policy 05-OIT-20, DRC IT Security Awareness Training.