SUBJECT: **Boundary Security**	PAGE 1 OF 5 .
	NUMBER: **05-OIT-03**
RULE/CODE REFERENCE:	SUPERSEDES: 05-OIT-03 dated 01/02/15
RELATED ACA STANDARDS:	EFFECTIVE DATE: **January 22, 2019**
	APPROVED:

Ohio | Department of Rehabilitation & Correction

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 boundary security guidelines to protect the Ohio Department of Rehabilitation and Correction (ODRC) system assets.

III. APPLICABILITY

This policy applies to all ODRC employees, contractors, volunteers, interns and other agents of the State.

IV. DEFINITIONS

Access Point - In this context, any point at which an entity outside the boundary connects to the network that contains secured assets.

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 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."

Boundary - The perimeter where security controls are in effect to protect secured assets.

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 (DAS OIT), 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 DRC information technology enterprise and to respond to system asset security incidents.

Consensus Audit Guidelines or CAG - A subset of information technology (IT) security controls in the National Institute of Standards and Technology (NIST) 800-53 publication, which addresses the highest threat areas for an organization's IT enterprise environment.

Intermediate Distribution Frame (IDF) - A cable rack that interconnects and manages telecommunications wiring between a main distribution frame (MDF) and workstation devices.

Firewall - Software or a combination of hardware and software that implements an operating system security policy governing traffic between two or more networks or network segments.

Main Distribution Frame (MDF) - 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 into a building with the internal network.

Packet - In networking, a packaging unit for transmitting data that has a defined header and data section. The header includes information for routing the packet to the intended destination.

Packet Filtering - A process that allows or denies an Internet Protocol ("IP") packet based upon criteria in the packet header.

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.

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.

Server - A computer that provides data, services and resources to other computers on a local area network (LAN) or a wide area network (WAN). Servers have many purposes and can exist as physical hardware or in a virtual machine (VM) environment.

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.

System Hardening - The process of enhancing the basic security layers associated with an application, firewall, and/or network~~.~~ to increase the level of system security against intrusion attempts.

Two-Factor Authentication - Authentication that incorporates two separate elements. An example is requiring both a password and a smart card.

V. POLICY

It is the policy of ODRC to adhere to all applicable ODRC IT security policies and DAS OIT Standard ITS-SEC-02, Enterprise Security Controls Framework, which emanate from the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Security and Privacy Controls for Federal Information Systems and Organizations, in order to safeguard and secure the boundary security of ODRC system assets, including ODRC MDFs, servers and ODRC IDFs, to ensure ODRC business continuity.

VI. PROCEDURES

1. The Bureau of Information Technology Systems (BITS) chief/designee, in consultation with the CISO, shall acquire, install, operate, and manage a boundary security capability, to include but not necessarily be limited to, ODRC MDFs, servers and IDFs located in ODRC facilities and offices, that satisfies ODRC's enterprise IT security requirements and complies with all applicable CAG controls and all applicable DAS OIT enterprise security controls framework standards.

2. When using another agency, vendors or contractors for Information Technology Service delivery or technical services programs or products, the DRC Chief of BITS, or designee, in consultation with the CISO, shall ensure that the providers, vendors or contractors deliver the boundary security precautions that satisfy ODRC's enterprise IT security requirements and all applicable DAS OIT enterprise security controls framework standards.

3. ODRC authorized users at the technical level shall follow the directions and instructions of the BITS chief/designee, and shall incorporate the approved IT system hardening techniques and automated tools, limit user access to necessary access points, and disable all other access points that conflict with any boundary security controls or standards promulgated by the BITS chief/designee.

4. In order to ensure the physical security of MDFs, servers and IDFs located in ODRC facilities and offices, the rooms and cages containing MDFs, servers and IDFs shall be secured with security locks and access to the rooms and cages shall be controlled as follows:

    a. Only authorized users at the technical level who are required to perform necessary IT duties and other ODRC employees who are required to perform necessary maintenance or security duties, as ~~and who are~~ approved by the managing officer/designee, shall have access to the rooms or cages. Authorized users at the technical level shall have access to the rooms or cages to perform their IT duties without the direct supervision of other ODRC employees. However, other approved ODRC employees who are required to perform maintenance or security duties in a locked room or cage shall be escorted into and out of the room or cage by an authorized user at the technical level who shall remain

in attendance in the room or cage until the required maintenance or security duties are completed.

b. Non-ODRC individuals, such as contractors, who are required to perform necessary IT or non-IT maintenance duties shall have access to the rooms or cages only upon receiving the advance approval of the managing officer/designee and only upon coordinating and scheduling the maintenance duties with the authorized user at the technical level. The approved non-ODRC individual shall be escorted into and out of the room or cage where maintenance is required by an authorized user at the technical level and shall be directly supervised by the authorized user at the technical level until the required maintenance is completed.

c. Access to rooms and cages containing MDFs, servers and IDFs shall be documented via the use of the DRC MDF/IDF/Server Room Sign-In/Sign-Out Log (DRC2190e).

i. One DRC MDF/IDF/Server Room Sign-In/Sign-Out Log (DRC2190e) shall be located in each room and cage.

ii. The DRC MDF/IDF/Server Room Sign-In/Sign-Out Log (DRC2190e) shall be completed by all individuals accessing the room and cage.

iii. The authorized user designated by the managing officer at the ODRC facility or office shall:

a) Visually inspect each DRC2190E at the facility or office on a weekly basis to ensure that individuals accessing each room and cage are entering all required information on the log form. During the visual inspections, the authorized user designated by the managing officer shall restock the log forms in the rooms and cages as necessary.

b) Collect the completed DRC2190E on a monthly basis, provide the log forms to the managing officer or designee and maintain a copy of the log form for audit purposes.

iv. Any violation of the use of the DRC2190E shall be reported via completion of a DRC Incident Report (DRC1000), pursuant to ODRC Policy 10-COM-08, Incident Reporting and Notification.

5. Authorized users at the technical level, including individuals that perform programming duties, shall use two-factor authentication to limit access to online ODRC information systems, resources and services that contain sensitive ODRC data, PII and other data whose disclosure would cause serious disruption or harm to State of Ohio business operations. Using the ODRC data identification and classification results, ODRC IT security risk assessments, the ODRC IT security plan and other available information, the BITS chief/designee, in consultation with the CISO, shall identify the online ODRC information systems that require two-factor authentication.

6. The BITS chief/designee, in consultation with the CISO and DAS OIT, shall identify the appropriate automated software tools to monitor, log and control network traffic, the frequency of said monitoring and logging, the storage and retention of monitoring and logging documentation and the ODRC authorized users at the technical level who shall be responsible for the monitoring, logging, controlling and documentation duties. In any case, all monitoring, logging, documenting and controlling of network traffic shall be completed pursuant to ODRC and DAS OIT IT security policies, standards, bulletins and directives and the standards promulgated by NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations.

7. The BITS chief, in consultation with the CISO, shall identify the appropriate software tools and ODRC authorized users at the technical level tasked to monitor, document, and log attempted or successful ODRC system asset probes, attacks or intrusions, including all repeated attempts from non-authorized entities to breach the boundary security. All monitoring, documenting and logging shall be completed pursuant to ODRC and DAS OIT security policies, standards, bulletins and directives and the standards promulgated by NIST Special Publication (SP) 800-53 Security and Privacy Controls for Federal Information Systems and Organizations. ODRC authorized users at the technical level assigned monitoring, documentation and logging duties shall report any evidence of an attack, probe or intrusion to the BITS chief and CISO via completion of a DRC Incident Report (DRC1000), pursuant to ODRC Policy 01-COM-08, Incident Reporting and Notification.

Related Department Forms:

Incident Report	DRC1000
DRC MDF/IDF/Server Room Sign-In/Sign-Out Log	DRC2190e