

STATE OF OHIO



DEPARTMENT OF REHABILITATION
AND CORRECTION

SUBJECT: Boundary Security	PAGE <u>1</u> OF <u>3</u> . NUMBER: 05-OIT-03
RULE/CODE REFERENCE:	SUPERSEDES: 05-OIT-03 dated 02/07/08
RELATED ACA STANDARDS:	EFFECTIVE DATE: January 2, 2015
	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 boundary security guidelines to protect the Ohio Department of Rehabilitation and Correction system assets.

III. APPLICABILITY

This policy applies to all Department 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.

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

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.

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.

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.

System Assets – Computer hardware, software, networks, data and/or other services or resources that are necessary to support the information technology requirements of the Ohio Department of Rehabilitation and Correction 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 the Ohio Department of Rehabilitation and Correction to adhere to all applicable CAG controls and the Ohio Department of Administrative Services, Office of Information Technology (DAS OIT) Standard ITS-SEC-02, Enterprise Security Controls Framework, in order to safeguard the boundary security of DRC system assets to ensure DRC business continuity.

VI. PROCEDURES

1. The DRC Chief of the Bureau of Information Technology Systems (BITS) shall acquire, install, operate, and manage a boundary security capability that 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 shall ensure that the providers, vendors or contractors deliver the boundary security precautions that satisfy DRC’s security needs.
3. DRC BITS technical staff shall incorporate approved system hardening techniques and automated tools, limit user access to necessary access points, and disable all other access points that conflict with boundary security controls or standards.
4. BITS technical staff, including programming staff, shall use two-factor authentication to limit access to online DRC information systems that contain DRC data requiring more secured access or information whose disclosure would cause serious disruption or harm to State business operations. The Chief of BITS shall identify the online DRC information systems that require two-factor authentication.
5. BITS technical staff shall incorporate the appropriate automated tools to monitor, log, and control network traffic.

6. DRC BITS technical staff shall monitor, document, and log attempted DRC system asset probes, attacks or intrusions, including all repeated attempts from non-authorized entities to breach the boundary security and shall report any evidence of an attack or intrusion to the DRC Chief of BITS via completion of a DRC Incident Report (DRC1000).

Related Department Forms:

Incident Report

DRC1000