

STATE OF OHIO



DEPARTMENT OF REHABILITATION
AND CORRECTION

SUBJECT: Malicious Software Code or Program Security Requirements	PAGE <u>1</u> OF <u>5</u>
	NUMBER: 05-OIT-18
RULE/CODE REFERENCE:	SUPERSEDES: 05-OIT-18 dated 08/06/14
RELATED ACA STANDARDS:	EFFECTIVE DATE: July 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 malicious software code or program security requirements to protect Ohio Department of Rehabilitation and Correction information technology system assets.

III. APPLICABILITY

This policy applies to all Ohio Department of Rehabilitation and Correction employees, contractors, volunteers, inmates, and other external individuals who have access to Ohio Department of Rehabilitation and Correction information technology system assets.

IV. DEFINITIONS

Anti-Virus Software - Computer software code or programs that prevent, detect, contain and remove malicious software codes or programs from a system asset. Anti-virus software is also called anti-malware.

Authorized User – A DRC employee, contractor, intern, volunteer or other agent of the state who is authorized at a high 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.

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.

Computer Virus - A form of a self-replicating malicious software code or program, usually invisible to an authorized user, that installs itself or a modified copy of itself on a system asset without the authorized user's consent with the intent of performing some type of harmful activity and when executed, "infects" one or more legitimate system asset codes or programs. Anti-virus software is used to detect, contain, and remove computer viruses.

Hacking - For the purposes of this policy, hacking is unauthorized access into a system asset with the intent of committing prohibited or malicious actions, such as viewing, copying or obtaining data without consent or installing a computer virus or other malicious software that can harm the system asset.

Malicious Software Code or Program - Any software code or program that is intentionally inserted or included into a system asset without the knowledge of the authorized user with the intention of controlling, disrupting, corrupting or otherwise causing harm, security breaches, or damage to the system asset. Malicious software codes or programs are also called malware, and examples include viruses, worms, Trojan horses, and trapdoors.

Phishing - An attempt via electronic communications, typically an e-mail, to obtain sensitive data, such as a computer user's usernames, passwords or other information, by posing as a trustworthy source such as a popular social web site, auction site, bank or online payment processor, IT technician/administrator, IT site, etc. Phishing e-mails contain downloadable malware or links to deceptive websites that often look and function like legitimate websites, but are infected with malware.

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 mobile removable readable or write-able computing data storage object, such as CD's, CD-R discs, DVD's, flash memory cards, USB jump drives and diskettes.

Reasonable Precaution - For the purposes of this policy, a reasonable precaution is a sound, rational, common sense action taken by an authorized user to prevent or avoid a harmful or undesirable information technology incident or result.

Record - Any item that is kept by DRC that: (1) is stored on a fixed medium, including an electronic or digital medium; (2) is created, received, or sent under the jurisdiction of DRC and (3) documents the organization, functions, policies, decisions, procedures, operations, or other activities of DRC.

Recovery - A defined step or process within an incident response plan with the goal of returning the affected or compromised systems to normal operations.

Sensitive Data - A record, information or data considered private, confidential or non-public, as prescribed by law, administrative rule or other legally binding authority, that access is restricted to a limited number of authorized DRC users for specialized business purposes and available only to non-DRC entities pursuant to a formal request, review and approval process, such as a Memorandum of

Understanding (MOU). Personal identification data, including an individual's last name, first name or first initial, in combination with any of the following data elements shall always constitute sensitive data: social security number, driver's license number, state identification card number, financial account number, credit card number, or debit card number. Sensitive data must be protected with a high level of security from unauthorized access, use, storage or release.

System Assets - Computer hardware, software, networks, data and/or 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.

V. POLICY

It is the policy of the Ohio Department of Rehabilitation and Correction (DRC) to protect its information technology system assets by establishing and managing computer system security requirements that prevent, detect, contain and remove malicious software codes or programs.

VI. PROCEDURES

A. The Office of Administration, Bureau of Information and Technology Services (BITS), is responsible for establishing and managing computer system security requirements throughout the DRC system asset enterprise that prevent, detect, contain and remove malicious codes or programs from DRC information technology system assets.

1. The Chief of BITS shall:

- a. Collaborate with the CISO to establish appropriate DRC information technology system asset standards, policies and procedures and communicate said standards, policies and procedures to BITS technical staff and DRC authorized users.
- b. Assign BITS technical staff from the Operation Support Center and regional locations to work with the CISO to prevent, detect, contain and remove malicious software codes or programs from DRC system assets.
- c. Ensure, through specific contractual stipulations, that all contractors providing information technology software services, resources, deliverables or products to DRC have procedures in place in their business to prevent, detect, contain and remove malicious software codes or programs from any software being used to generate or provide information technology software services, resources, deliverables or products to the Department.
- d. Immediately report serious or major malicious code and program security breaches or outbreaks that occur throughout the DRC information technology enterprise to the Deputy Director of the Office of Administration and other DRC administrators as appropriate.

2. The CISO shall:

- a. On an ongoing basis, establish malicious code or program system security requirements and protection standards for all DRC information technology system assets, including mobile data storage devices, such as flash drives and diskettes and

present said requirements and standards to the Chief of BITS and to all other DRC technical staff.

- b. On an annual basis, assess the DRC's requirements and needs for anti-virus protection at the enterprise level and present the findings to the Chief of BITS and to all other DRC technical staff.
 - c. On an annual basis, complete a plan for the purchase and deployment of necessary anti-virus software required to protect DRC information technology system assets and present the plan to the Chief of BITS and to all other DRC technical staff.
 - d. Immediately report serious or major malicious code and program security breaches or outbreaks that occur throughout the DRC information technology enterprise to the Chief of BITS and secure and maintain the evidence or documentation of the serious or major security breach or outbreak for the appropriate administrative or law enforcement authorities.
 - e. On an ongoing basis, collect information about less major or less serious outbreaks of malicious software codes or programs that occur throughout the DRC information technology enterprise and the action taken to prevent, detect, contain and remove the malicious software codes and programs. This information shall be maintained and shall be provided at regular intervals to the Chief of BITS.
 - f. Maintain knowledge and expertise in enterprise information technology security system requirements and standards, including knowledge and expertise in the most current anti-virus software.
 - g. Give system security direction and guidance to BITS technical staff members at the Operation Support Center and to other technical staff members deployed throughout the Department.
3. BITS technical staff shall at regular intervals as directed by the CISO
- a. Check for updates to anti-virus protection software and, when new updates are released, install the updates without delay on DRC computing devices and servers.
 - b. Check all DRC computing devices, including mobile data storage devices, to prevent, detect, contain, and remove malicious software codes or programs before issuing the computing devices to Department employees, contractors, volunteers and inmates.
 - c. Ensure all software installed on DRC computing devices or servers, including software developed internally, is free from malicious software codes or programs before the software is installed on a DRC computing device or server.
 - d. Conduct scans of DRC mobile computing devices, such as laptops and tablets, to identify mobile computing devices that have not received the required anti-virus software updates, and disable the devices until they can be properly checked for malicious software codes or programs.

- e. Conduct scans of file transfer programs sent to or from the DRC to ensure that they are free of malicious software codes or programs.
- B. Each DRC employee, contractor, volunteer, inmate, and any other external individual with access to DRC information technology system assets is responsible for:
1. Following all applicable DRC information technology policies.
 2. Maintaining awareness of malicious code and program risks and taking reasonable precautions to protect and safeguard DRC system assets, especially DRC records and DRC sensitive data. Reasonable precautions include, but are not limited to, being careful with e-mails by opening only e-mails, e-mail attachments and links with e-mails that have been sent by known and trusted sources.
 3. Not distributing malicious code or programs.
 4. Using only appropriate and approved portable computing devices and portable computing media.
 5. Not disabling or tampering with any anti-virus software that is installed on a DRC information technology system asset.
 6. Reporting any malicious code or program encountered while using a DRC information technology system asset to the appropriate supervising authority, Chief of BITS and the CISO as a Special Incident, pursuant to Department Policy 01-COM-08, Incident Reporting and Notification.