

SUBJECT: DRC Information Technology Security Awareness Training	PAGE <u> 1 </u> OF <u> 3 </u>
	NUMBER: 05-OIT-20
RULE/CODE REFERENCE:	SUPERSEDES: 05-OIT-20 dated 09/13/11
RELATED ACA STANDARDS:	EFFECTIVE DATE: October 14, 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 Ohio Department of Rehabilitation and Correction (DRC) information technology security awareness training guidelines that meet the requirements established by the Department of Administrative Services Office of Information Technology (DAS – OIT) Policy IT-15, IT Security Awareness and Training which is derived from NIST Special Publication 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013.

III. APPLICABILITY

This policy applies to all employees of the Ohio Department of Rehabilitation and Correction (DRC) and other individuals, such as DRC contractors and DRC volunteers, who by virtue of their job duties, roles, responsibilities, or assignments have access to DRC information technology system assets.

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.

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.

Role-Based IT Security Training - Targeted IT security awareness training that strives to produce relevant and necessary security knowledge and skills within the DRC workforce. The training provides designated DRC employees and other individuals that have access to DRC system assets with an in-depth competency development associated with specific DRC IT security roles and specific access to DRC system assets. An online training program is preferable, because it is standardized, readily available and generates appropriate training documentation. However, this training may also be conducted in other more traditional training formats approved by DRC.

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 to protect DRC information technology system assets by delivering Basic IT Security Awareness Training, Role-Based IT Security Training and other necessary IT security awareness training to DRC authorized users per the DAS – OIT requirements mandated in DAS – OIT Policy IT-15, IT Security Awareness and Training which is derived from NIST Special Publication 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013.

VI. **PROCEDURES**

- A. Pursuant to DAS – OIT Policy IT-15, IT Security Awareness and Training, the DAS Office of Information Security and Privacy (OISP) shall:
1. Provide DRC with the appropriate and current training information, materials or solutions so DRC may conduct Basic Information IT Security Awareness Training.
 2. Update the training information, materials or solution on an annual basis to ensure it remains current and addresses the latest IT security threats and best practices.
- B. New DRC employees shall successfully complete DRC Basic IT Security Awareness Training during DRC New Employee Orientation (NEO) or during employee orientation at the worksite. Prior to approving the employee's DRC system access, the immediate supervisor shall verify the training was successfully completed by reviewing the employee's training record.

- C.** New DRC contractors, volunteers and other authorized users shall receive a contingency worker account to access online training and shall successfully complete DRC Basic IT Security Awareness Training during the required orientation at the worksite. Prior to approving the individual's DRC system access, the immediate supervisor shall verify the training was successfully completed by reviewing the individual's training record.
- D.** All authorized users shall successfully complete ongoing DRC's required Basic IT Security Awareness Training:
1. On an annual basis during DRC's in-service training cycle in order to retain their DRC system access. The immediate supervisor shall verify the training was successfully completed by reviewing training records and, when records indicate that an authorized user did not successfully complete the training, the immediate supervisor shall take the appropriate steps to terminate the authorized user's DRC system access. DRC system access shall not be restored to the authorized user until the training is successfully completed and verified by the immediate supervisor.
 2. When a change in their DRC responsibilities or roles occurs that necessitates a required change in their DRC system access. Prior to approving the authorized user's change in DRC system access, the immediate supervisor shall verify the authorized user successfully completed the required DRC Basic IT Security Awareness Training by reviewing the training record.
- E.** All authorized users shall complete any supplemental IT security training required by the DRC Chief of the Bureau of Information Technology Services (BITS) to address new best practices, DRC-specific IT security requirements or new laws or regulations that impact DRC operations. The DRC Chief of BITS/designee shall coordinate the scheduling of the training with the DRC Chief Information Security Officer (CISO) and superintendent of the Corrections Training Academy/designee and the training shall be delivered and documented pursuant to all applicable DRC training standards.
- F.** Authorized DRC users that have unique responsibilities or roles for protecting DRC system assets, such as authorized users at the technical level, IT system administrators and database administrators, senior administrators and data owners and application developers/programmers shall complete any Role-Based IT Security Training required by the DRC Chief of BITS. The Chief of BITS/designee shall coordinate the scheduling of the training with the DRC CISO and superintendent of the Corrections Training Academy/designee and the training shall be delivered and documented pursuant to all applicable DRC training standards.
- G.** Authorized user training records shall be maintained in accordance with DRC record retention requirements to ensure that Basic IT Security Awareness Training and Role-Based IT Security Training are being fulfilled.