

STATE OF OHIO



DEPARTMENT OF REHABILITATION
AND CORRECTION

SUBJECT: DRC Information Technology Security Risk Assessments	PAGE <u>1</u> OF <u>4</u>
	NUMBER: 05-OIT-27
RULE/CODE REFERENCE:	SUPERSEDES: NEW
RELATED ACA STANDARDS:	EFFECTIVE DATE: August 25, 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 for Ohio Department of Rehabilitation and Correction (DRC) formal information technology system asset security risk assessments pursuant to the requirements of the Ohio Department of Administrative Services, Office of Information Technology Policy ITS-SEC-02, which is derived from NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations.

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 volunteers, who have access to DRC information technology (IT) system assets.

IV. DEFINITIONS

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.

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

DRC Information Technology Governance Group (ITGG) - The multi-disciplinary leadership group, chaired by the Deputy Director of the Office of Administration and comprised of DRC executive staff and administrators from the Office of Administration Bureau of Information Technology Services (BITS), charged with approving and prioritizing all enterprise DRC IT projects, approving security standards and requirements for all DRC IT system assets as presented by the DRC CISO and guiding DRC's information technology biennial plan to ensure that information technology system assets are identified, obtained, secured and utilized in an efficient and effective manner to achieve and sustain DRC's mission and business continuity.

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 (DRC) 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 DRC IT system assets by conducting formal IT security risk assessments under the oversight of the DRC CISO pursuant to the requirements of the Ohio Department of Administrative Services, Office of Information Technology Policy ITS-SEC-02, which is derived from NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations.

VI. PROCEDURES

A. The DRC CISO shall be responsible for:

1. Developing DRC data security classification guidelines and standards for all manual and automated DRC information/data types, such as documents, data records, online data systems and data files, promulgating the standards to the Director, DRC managing directors, the chief of BITS, the ITGG and other DRC administrators, and auditing compliance for said standards at regular intervals as approved by the DRC chief of BITS.
2. Identifying the appropriate software tools, procedures and/or other security controls to complete DRC IT security risk assessments to protect DRC system assets.
3. Administering the appropriate automated or manual vulnerability scanning of DRC system assets, to be prioritized by risk, to include implementing standardized quarterly vulnerability scanning schedules and additional ad hoc vulnerability scanning, as necessary, establishing threat detection and categorization thresholds, reporting scanning findings and results and requiring the appropriate actions to remediate or mitigate any risks discovered during scanning.
4. Completing DRC IT security risk assessments annually or as required by the chief of BITS to protect all DRC system assets and when significant changes occur in the DRC information systems. The CISO has the authority to secure the assistance of DAS – OIT, BITS staff and operations staff in DRC facilities and offices to complete said IT security risk assessments.

5. Reporting all DRC IT security risk assessment results, findings and recommendations for remediation to the Director, the managing directors, the chief of BITS, the ITGG and other DRC administrators and DAS – OIT. The results of risk assessments will determine appropriate priorities for and remediation actions that must be taken in implementing the necessary security controls.
 6. Reviewing all DRC IT projects associated with DRC system assets in order to:
 - a. Identify and require the appropriate security controls for any enterprise project presented to or approved by the DRC ITGG
 - b. Pause or terminate other DRC IT projects, not presented to or approved by the DRC ITGG, if it is determined that the project lacks appropriate security controls and, therefore, represents a security risk to DRC system assets.
 7. Reviewing all DRC enterprise system asset contracts and enterprise system asset purchases, via information provided by the staff of the DRC Office of Administration, to ensure that the products or services being acquired by DRC contain the appropriate security controls to protect DRC system assets.
 8. Reviewing all DRC IT policies at designated intervals to ensure the policies align with the most current best practices in IT security controls.
 9. Recommending appropriate security awareness training for DRC employees, contractors, volunteers and other individuals that are authorized to have access to DRC system assets.
- B. DRC IT security risk assessments should balance the requirements for appropriate security controls necessary to protect DRC system assets and DRC’s business requirements related to the creation, storage, transmission and storage of data and other information. Internal and external security risk assessments conducted by the DRC CISO must also take into account changing organizational priorities and the fluid nature of threats targeting DRC’s system assets. As a result, security risk assessments conducted by the DRC CISO must involve the systematic consideration of the following factors:
1. The nature of DRC system asset being assessed.
 2. The business purpose for which the DRC system asset is intended and used.
 3. The environment in which the DRC system asset is used, operated and maintained.
 4. The base protections already in place for the DRC system asset.
 5. The organizational appetite for risk and the vulnerabilities that will likely result from a significant breach of DRC security, taking into account possible consequences of failure of information confidentiality, integrity and availability.

6. The realistic likelihood of such a DRC security breach occurring in light of the prevailing threats and controls.
 7. The level of security controls necessary to remove, reduce or mitigate the risk, keeping in mind that the level of security controls for DRC system assets will increase as the level of vulnerability and risk increase.
- C. The DRC CISO will update the risk assessment whenever there are significant changes to the information systems or the operational environment, including discovery of new threats and vulnerabilities or when other conditions occur that pose a risk or impact the security state of the information system.
- D. At the conclusion of the DRC vulnerability scanning cycle, the DRC CISO will review and accredit the remaining known DRC system asset vulnerabilities to ensure they pose an acceptable residual level of risk to DRC business operations and DRC system assets, and provide the results, findings and recommendations of the authorization process to the chief of BITS, the DRC ITGG, other DRC administrators and DAS – OIT.