

STATE OF OHIO



DEPARTMENT OF REHABILITATION  
AND CORRECTION

SUBJECT: <b>DRC Information Technology Security Assessment &amp; Authorization</b>	PAGE <u>1</u> OF <u>4</u>
	NUMBER: 05-0IT-26
RULE/CODE REFERENCE:	SUPERSEDES: New
RELATED ACA STANDARDS:	EFFECTIVE DATE: September 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 guidelines for Ohio Department of Rehabilitation and Correction (DRC) information technology security assessment and authorization process pursuant to the requirements of the Ohio Department of Administrative Services, Office of Information Technology State IT Standard 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 DRC volunteers who have access to DRC information technology 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 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 utilize appropriate IT security assessments and authorization, under the oversight of the DRC CISO, pursuant to the requirements of the Ohio Department of Administrative Services, Office of Information Technology State IT Standard ITS-SEC.02, which is derived from NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, to protect the security of DRC IT system assets.

## VI. PROCEDURES

A. The DRC CISO shall be responsible for:

1. Identifying the appropriate automated and manual tools to complete annual DRC IT security assessments and authorizations.
2. Utilizing the DRC Critical Controls Assessment in combination with the DRC Internal Management Audit on an annual basis to encompass the annual DRC enterprise security assessment plan that details the scope of the assessment and authorization process including the timelines for completing the assessments, a description of the DRC environments being assessed, a list of the DRC system asset security controls and control enhancements being assessed, the assessment procedures to be used to test and determine the security control effectiveness, the composition, roles and responsibilities of the DRC security assessment team and the assessment format that documents assessment findings, results and recommendations for remediation.
3. Presenting the annual DRC enterprise security assessment plan to the DRC ITGG for their review and approval.
4. Directing the DRC security assessment team, which shall be comprised of DRC IT staff, DAS – OIT staff and other individuals deemed appropriate for the team, in the completion of the annual security assessments.

5. Reviewing the findings, results and recommendations submitted by the DRC security assessment team and formulating the action plan to remediate the issues and apply the appropriate security controls to address the team recommendations.
6. Reporting all DRC security assessment results, findings, and action plans to the Director, the Managing Directors, the Chief of BITS, the ITGG, other DRC administrators and DAS – OIT. The results of the assessments will determine appropriate priorities to be taken in implementing the action plan.
7. Directing implementation of all DRC security assessment action plans, utilizing DRC IT staff, DAS – OIT and other technical resources as necessary.
8. Reviewing with DRC legal section staff, DRC BITS staff, DRC data owners and the DRC ITGG, all electronic and manual data sharing memorandum of understandings (MOUs) to be executed between DRC and external organizations to ensure that the appropriate data security requirements are specified to protect the DRC data. Said MOUs, which shall serve as the formal authorization for the data sharing, shall specify the data security conditions and requirements, such as data ownership; responsibilities for data protection; technical requirements for the data transmission; technical requirements for the recording, reading and storage of the data; management responsibilities for controlling and notifying data transmission and data receipt; procedures for the notifying of data transition and receipt; minimum acceptable technical standards for data packaging and transmission; data courier identification requirements; responsibilities and liabilities in the event of data corruption or data loss and any special measures required to protect sensitive data, such as encryption keys.
9. Administering DRC’s information security authorization program, which shall include certifying existing DRC system asset security controls on an annual basis, to ensure that the system controls have been properly implemented and are operating as prescribed with minimal risk and producing the desired results; accrediting 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 providing the results, findings and recommendations of the authorization process to the Director, the Managing Directors, the Chief of BITS, the DRC ITGG, other DRC administrators and DAS – OIT.
10. Administering the security authorization process, to include coordinating annual testing certification with DRC data owners, DRC programming staff and, if appropriate, external software vendors completing programming projects for DRC; developing and monitoring action plans, in consultation with the DRC data owners, to remediate vulnerabilities; conducting the accreditation process, in consultation with the DRC data owners, to determine if the remaining known vulnerabilities in the information system pose an acceptable level of risk to DRC business operations and system assets and providing the DRC Chief of BITS with an annual briefing containing the results of the updated privacy assessment, updated system security plan, updated security risk assessment, security tests and evaluations and the status of any outstanding security action plans that address the remediation of known vulnerabilities.

11. Administering the process that encompasses the ongoing monitoring of DRC system assets, through quarterly vulnerability scanning, assignment of priorities to detected vulnerabilities, the documentation and tracking of non-compliance and resulting remediation and mitigation actions and the reporting of vulnerability management conditions to the DRC ITGG for the review and approval of action plans to address non-compliance, risk management strategies and decisions so as to facilitate the awareness of threats, vulnerabilities and information security to support DRC's system asset risk management decisions.