

<b>SUBJECT:</b> <b>DRC Information Technology Security Plan</b>	PAGE <u>  1  </u> OF <u>  5  </u>
	NUMBER: <b>05-OIT-28</b>
<b>RULE/CODE REFERENCE:</b> NIST SP 800-53, Security Planning Control	<b>SUPERSEDES:</b> New
<b>RELATED ACA STANDARDS:</b>	<b>EFFECTIVE DATE:</b> October 28, 2016
	<b>APPROVED:</b> 

## 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 procedures to protect Ohio Department of Rehabilitation and Correction (DRC) system assets by completing a written annual information technology (IT) security plan that meets the security planning requirements of the Ohio Department of Administrative Services, Office of Information Technology (DAS OIT), which are derived from the National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations.

## III. APPLICABILITY

This policy applies to all DRC authorized users who have access to DRC 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 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.

**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 the responsibility of guiding DRC's information technology biennial plan to ensure that information technology system assets are identified, obtained and utilized in an efficient and effective manner to achieve and sustain DRC's mission and business continuity.

**Information Technology (IT) Security Plan** - A written document completed on an annual basis that contains information about DRC's IT security requirements and DRC's existing IT security controls as well as recommendations and action plans for improving DRC IT security controls to protect DRC system assets.

**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 system assets by completing a written annual IT security plan that meets the security planning requirements of DAS OIT, which are derived from the NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations.

## VI. PROCEDURES

- A. On an annual basis, the chief of the BITS and the CISO shall convene a multi-disciplinary DRC IT security planning group to collect and compile information to prepare the annual DRC IT security plan. The group shall include, but is not necessarily limited to, the following members:
1. Data owners or their designees;
  2. Authorized users at the end user level, representing DRC and external end users;
  3. Authorized users at the technical level, representing the various technologies of IT staff assigned to BITS and DRC facilities; and
  4. Representatives from external organizations that manage or co-manage DRC system assets or who have a significant stake in the security of DRC's system assets.
- B. The CISO and chief of BITS shall co-chair the IT security planning effort and, in doing so, shall exercise the following duties:
1. Establish necessary committees and select members of the IT security planning group, and others as necessary, to serve on said committees;

2. Conduct all general IT security planning meetings and document said meetings with written agendas and attendance sheets and a written record of meeting proceedings and decisions; and
  3. Complete and distribute the annual IT security plan.
- C. As part of the planning effort leading to completion of the annual IT security plan, the IT security planning group shall collect/compile a variety of information related to the security requirements and status of DRC's IT enterprise, such as:
1. A summary of DRC's existing IT enterprise, including a list of DRC's system assets and a list of authorized users at the technical level that administer, support and maintain the IT enterprise.
  2. A list of DRC's primary information systems with an explanation of the operational environment of each system, including the mission and business processes of each system, and each system's relationship with or connection to other information systems.
  3. Copies of the privacy impact assessments for new or changed DRC information systems that have been completed since completion of the last IT security plan.
  4. A description of the IT security controls mandated by statute, administrative rules and regulations, NIST, DAS OIT and other sources identified by the CISO as required to protect DRC's existing system assets.
  5. An overview of DRC's existing IT security architecture and framework and authorization boundary for the system, including a description of the responsibilities and expected behaviors of all authorized users who access DRC system assets.
  6. A summary of the results of all IT-related DRC internal management audits completed since completion of the last annual IT security plan.
  7. A description of any IT security incidents since completion of the last annual IT security plan that required a response pursuant to DRC policy 05-OIT-14, Information Technology Security Incident Response.
  8. A summary of the annual review of the DRC IT audit process, completed by the CISO pursuant to DRC policy 05-OIT-28, DRC Information Technology Audit and Accountability Procedures, since completion of the last annual IT security plan.
  9. The data access qualification guidelines and data compliance reviews completed by data owners and the CISO during the last annual compliance review, pursuant to DRC policy 05-OIT-23, DRC Data Identification and Classification Requirements.
  10. A summary of the DRC information technology security risk assessments completed by the CISO since the last annual IT security plan.

11. A description of the existing IT governance process used within DRC to identify, review, prioritize, approve, fund and procure necessary, cost-effective IT security protection and controls for all DRC system assets and a summary of the IT security protection and controls procured to protect DRC system assets since completion of the last annual IT security plan.
  12. An assessment of the extent to which DRC's existing IT security controls meet DRC's existing IT security framework requirements, including a description of the gaps between the existing IT security framework and existing IT security controls.
  13. Relevant IT security input from:
    - a. The various internal and external levels of authorized users at the end user level;
    - b. The various levels of authorized users at the technical level; and
    - c. External organizations that manage or co-manage DRC system assets or that have significant stake in the security of DRC's system assets.
- D. Upon completion of all IT security planning activities by the IT security planning group, the chief of BITS and CISO shall prepare a written annual DRC IT security plan, which shall contain, at a minimum:
1. A review of the information collected/compiled by the IT security planning group during the annual IT security planning effort;
  2. The findings of the IT security planning group as to the existing security status of DRC's IT enterprise, as derived from the information collected/compiled by the IT security planning group during the annual IT security planning effort; and
  3. Recommendations and action plans for improving DRC IT security controls to better protect DRC system assets.
- E. The chief of BITS and CISO shall present the draft written annual DRC IT security plan to the data owners and other appropriate administrators for their review of the findings and approval of the recommendations and action plans.
- F. When the annual DRC IT security plan is finalized by the data owners, the chief of BITS and CISO shall submit the plan to the Director and other internal and external individuals as deemed appropriate.
- G. The chief of BITS and CISO shall be responsible for ensuring that the action plans developed to address the recommendations in the annual DRC IT security plan are:
1. Assigned for completion to the appropriate DRC authorized users at the technical level;
  2. Monitored at regular intervals to ensure progress is being made in completing the plans; and

3. Successfully completed pursuant to the action plan timeframes.
- H. The chief of BITS or CISO shall provide reports about the status of the action plan at regular intervals to the ITGG.