

	State of Indiana Indiana Department of Correction	Effective Date	Page 1 of	Number
		12/1/2020	5	04-05-106
<p>POLICY AND ADMINISTRATIVE PROCEDURE Manual of Policies and Procedures</p>				

Title ANNUAL INFORMATION TECHNOLOGY SECURITY PLAN

Legal References (includes but is not limited to)	Related Policies/Procedures (includes but is not limited to)	Other References (includes but is not limited to)
11-8-5-2	04-03-101 04-03-103 04-03-111	NIST 800-53 Rev 4

I. PURPOSE:

The purpose of this policy is to establish procedures to protect the Indiana Department of Correction system assets by completing a written annual information technology (IT) security plan that meets the security planning requires of the Indiana Office of Technology (IOT) 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.

II. POLICY STATEMENT:

It is the policy of the Indiana Department of Correction to protect IDOC system assets by completing a written annual IT security plan that meets the security planning requirements of the Indiana Office of Technology, which are derived from the NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations. This policy and administrative procedure shall be reviewed annually and updated as necessary.

III. DEFINITIONS:

For the purpose of this policy and administrative procedure, the following definitions are presented:

- A. **AUTHORIZED USER:** An IDOC employee, contractor, intern, volunteer or other agent of the State who is authorized at a technical level to administer and support/maintain state computing IT systems or is authorized at an end user level, to have access to and use State computing IT systems and telecommunications technology systems for business purposes on behalf of the State of Indiana.

POLICY AND ADMINISTRATIVE PROCEDURE

Indiana Department of Correction

Manual of Policies and Procedures

Number	Effective Date	Page	Total Pages
04-05-106	12/1/2020	2	5
Title			
ANNUAL INFORMATION TECHNOLOGY SECURITY PLAN			

- B. **INFORMATION SECURITY OFFICER:** The technical staff members assigned to the Technology Services Division (TSD) that, in collaboration with the Indiana Office of Technology, Executive Director of Technology Services, and other TSD technical staff members, is response for the security oversight of IDOC’s IT system assets by establishing appropriate system asset security standards and risk controls to identify, develop, implement, maintain and support security process across the IDOC IT enterprise and to respond to system asset security incidents.
- C. **DATA OWNERS:** IDOC managing directors or designees that are authorized users responsible for identifying and classifying data for their respective areas.
- D. **IT (IT) SECURITY PLAN:** A written document completed on an annual basis that contains information about IDOC’s IT security requirements and IDOC’s existing IT security controls as well as recommendations and action plans for improving IDOC IT security controls to protect IDOC system assets.
- E. **SYSTEM ASSETS:** Computer hardware, software, networks, data and/or services or resources that are necessary to support the IT requirements of the Indiana Department of Correction and therefore, must be protected by the appropriate security requirements to ensure business continuity.

IV. PROCEDURES:

- A. On an annual basis, the Executive Director of Technology Services and the Information Security Officer shall convene a multi-disciplinary IT security planning group to collect and compile information to prepare the annual IT security plan. The group shall include, but is not necessarily limited to, the following members:
 - 1. Data owners or designees;
 - 2. Authorized users at the end user level, representing facilities and external users;
 - 3. Authorized users at the technical level, representing TSD and facilities; and,
 - 4. Representatives from external organizations that manage or co-manage IDOC system assets or who have a significant stake in the security of IDOC system assets.
- B. The Information Security Officer and the Executive Director of Technology Services 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;

POLICY AND ADMINISTRATIVE PROCEDURE

Indiana Department of Correction

Manual of Policies and Procedures

Number	Effective Date	Page	Total Pages
04-05-106	12/1/2020	3	5

Title
ANNUAL INFORMATION TECHNOLOGY SECURITY PLAN

2. Conduct all general IT security planning meetings and document said meetings with written agendas, attendance sheets and a written record of meeting proceedings or 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 IDOC’s IT enterprise, such as:
1. A summary IDOC’s IT enterprise, including a list of IDOC’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 IDOC’s primary information systems with an explanation of the operational environment of each system, including the mission and business process of each system, and each system’s relation with or connection to other information systems;
 3. Copies of any impact assessments for new or changed IDOC information systems that have been completed since completion of the last IT security plan;
 4. A description of the IT security controls, and all baseline configuration requirements mandated by statute, administrative rules, and regulations, NIST, IOT, and other sources identified by the Information Security Officer as required to protect IDOC’s existing system assets;
 5. An overview of IDOC’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 IDOC system assets; and
 6. A description of any IT security incidents since completion of the last annual IT security plan.
- D. Upon completion of all IT security planning activities by the IT security planning group, the Executive Director of Technology Services and the Information Security Officer shall prepare a written annual IDOC 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;

POLICY AND ADMINISTRATIVE PROCEDURE

Indiana Department of Correction

Manual of Policies and Procedures

Number	Effective Date	Page	Total Pages
04-05-106	12/1/2020	4	5

Title

ANNUAL INFORMATION TECHNOLOGY SECURITY PLAN

2. The findings of the IT security planning group as to the existing security status of IDOC's IT enterprise, as derived from the information collected/compiles by the IT security planning group during the annual IT security planning effort;
 3. Recommendations and action plans for improving IDOC IT security controls to better protect IDOC system assets;
 4. Incident reporting procedures;
 5. Staff roles and responsibilities for incident response and management;
 6. Incident investigation procedures;
 7. Incident remediation and closure procedures; and,
 8. Post-incident review and action planning procedures that focus on preventing future occurrences.
- E. The Executive Director of Technology Services and the Information Security Officer shall present the draft written annual IDOC 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 IDOC IT security plan is finalized by the data owners, the Executive Director of Technology Services and Information Security Officer shall review the plan and share as appropriate with internal and external individuals.
- G. The Executive Director of Technology Services and Information Security Officer shall be responsible for ensuring that the action plans developed to address the recommendations in the annual IDOC IT security plan are:
1. Assigned for completed to the appropriate IDOC authorized user 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 Executive Director of Technology Services or Information Security Officer shall provide reports about the status of the action plan at regular intervals, to senior Department leadership.

POLICY AND ADMINISTRATIVE PROCEDURE

Indiana Department of Correction

Manual of Policies and Procedures

Number	Effective Date	Page	Total Pages
04-05-106	12/1/2020	5	5
Title			
ANNUAL INFORMATION TECHNOLOGY SECURITY PLAN			

XIV. APPLICABILITY:

This policy and administrative procedure is applicable to all Department facilities, staff, and offenders, except those offenders on Parole, and to those facilities that are operating under a court order or consent decree that mandates different procedures.

signature on file
Robert E. Carter, Jr.
Commissioner

_____ Date