State of Indiana
Indiana Department of Correction

Effective Date	Page 1 of	Number
12/1/2020	4	04-05-105

POLICY AND ADMINISTRATIVE PROCEDURE

Manual of Policies and Procedures

Title

INFORMATION TECHNOLOGY SECURITY INCIDENT RESPONSE

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	IOT-CS-SEC-132 IOT-CS-SEC-133

I. PURPOSE:

The purpose of this policy and administrative procedure is to establish the Indiana Department of Correction (IDOC) information technology (IT) security incident response team and the standardized procedures for responding to any IT security and/or privacy incidents in order to protect IDOC System Assets pursuant to the requirements of the Indiana Office of Technology which are derived from 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 utilize an IDOC IT security incident response team, and standardized procedures for responding to IT Security Incidents based upon an annual Security Plan, in order to protect IDOC System Assets pursuant to the requirements of the Indiana Office of Technology, which are derived from National Institute of Standards and Technology (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. ATTACK VECTORS: A path or means by which a hacker can gain access to a computer or network server in order to deliver a malicious payload, such as a virus, a Trojan horse, a worm, or spyware. Attack vectors enable hackers to exploit system vulnerabilities, including the human element. Common attack vectors include, but are not limited to:

- External/removal media - An attack executed via removal media, such as an infected USB flash drive.

- Web - An attack executed from a Web site or Web-based application, such as a cross-site scripting attack used to steal user credentials or a redirect to a site that exploits a browser vulnerability and installs malware.

- E-mail - An attack executed via an e-mail message or e-mail attachment, such as an exploit code disguised as an attached document or a link to a malicious Web site in the body of an e-mail message.

- Impersonation - An attack involving the replacement of something benign with something malicious, such as spoofing, man in the middle attacks, rogue wireless, access points and SQL Injections.

- Improper Usage - Any incident resulting from violation of an organization's acceptable usage policies by an Authorized User, such as an Authorized User performing in illegal activities on an information system or an Authorized User installing file sharing software on an organization's network, leading to the loss of sensitive data.

- Loss or Theft - The Loss or Theft of a computing device or media used by the State agency, such as a laptop, smartphone, tablet, etc. This also includes loss or theft of hard copy documents that contain sensitive data or PII.

B. 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 information 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 Indiana.

C. AVAILABILITY: The ensuring of timely and reliable access to and use of information.

D. CONFIDENTIALITY: Preserving authorized restrictions on information access and disclosure, including the means for protecting privacy and proprietary information.

E. CONTINGENCY OPERATIONS: The organized response/handling by the IDOC IT security incident response team, pursuant to the annual contingency plan, of serious information technology security or privacy incidents that result in significant IDOC enterprise disruption, compromise, or failure of any system asset.

F. CONTINGENCY PLAN: A written document completed on an annual basis by the IDOC that identifies the IT requirements necessary to ensure IDOC's business continuity in the event that a serious information technology security incident results in significant IDOC enterprise disruption, compromise or failure of any system asset that necessitates activation of the Contingency Plan and initiation of a Contingency Operation.

G. DATA CUSTODIAN: IDOC authorized users at the technical level responsible for the safe custody, transport, and storage of state data as well as the implementation of any applicable federal, state, or agency data protection requirements.

H. DATA OWNERS: IDOC managing directors or designees that are authorized users responsible for identifying and classifying data for their respective areas.

I. DENIAL OF SERVCE (DoS): An attack on systems assets that successfully prevents or impairs the normal authorized functionality of networks, systems, or applications by exhausting resources. Examples include, but are not limited to:

- Attacks that adversely affect or degrade access to critical services.
- Persistent or significant DoS attacks (e.g., attempted DoS attacks aimed specifically at DNS servers or routers.
- Use of state computing device to initiate or facilitate a distributed DoS attacks or DDoS attacks.
- Failed or successful attempts to cause failures in critical infrastructure services, loss of critical supervisory control and data acquisition systems or services (SCADA).

J. DISTRIBUTED DENIAL OF SERVICE (DDoS): A denial of service (DoS) technique that uses numerous hosts to perform the attack on system assets.

K. INFORMATION SECURITY OFFICER (ISO): The technical staff member of IDOC that, in collaboration with the Indiana Office of Technology, Executive Director of Technology Services, and other IDOC technical staff members, is responsible for the security oversight of IDOC'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 IDOC information technology resources and to respond to system asset security incidents.

IV. PROCEDURES:

A. Indiana DOC shall maintain an IT security incident response team, which shall be comprised of the following representatives:

1. The Executive Director of Technology Services, who shall co-chair the team;
2. The Information Security Officer, who shall co-chair the team;
3. Staff members from the Technology Services Division (TSD) and additional Authorized Users at the technical level, selected by the Executive Director of Technology Services;
4. A representative from the Legal Services Division, selected by the Chief Legal Officer;
5. A representative from the Communications Division, selected by the Chief of Communications; and,
6. Representatives from the impacted data owners, when the team is activated to respond to an IT security incident.

B. The IDOC IT security incident response team shall be responsible for:

1. Maintaining a current list of all Authorized Users at the technical level in TSD and in the facilities that may be called upon to respond when an incident occurs. The list shall include business and personal contact information and a summary of the user' technical training, expertise and skills.

2. Providing guidance to Authorized Users at the technical level in TSD and in facilities/regions to assist them in performing the appropriate duties, tasks and activities necessary to support IDOC IT Security Incident assessment, evaluation, analysis, response and follow-up.

3. Meeting at regular intervals as determined by the team co-chairs. Meetings shall be documented with agendas, attendance sheets, and written notes summarizing the topics discussed and decisions made during the meeting.

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. Date
Commissioner