

STATE OF OHIO



DEPARTMENT OF REHABILITATION
AND CORRECTION

SUBJECT: Information Technology Security Incident Response	PAGE <u>1</u> OF <u>11</u>
	NUMBER: 05-OIT-14
RULE/CODE REFERENCE: Ohio DAS Policy ITP-B.1; B.7 & ITS-SEC.02	SUPERSEDES: 05-OIT-14 dated 04/20/09
RELATED ACA STANDARDS:	EFFECTIVE DATE: August 31, 2016
	APPROVED: 

I. AUTHORITY

This policy is issued in compliance with Ohio Revised Code 5120.01 which delegates to the Director of the Ohio 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 the Ohio Department of Rehabilitation and Correction (DRC) information technology (IT) security incident response team and the standardized procedures for responding to IT security incidents in order to protect DRC system assets pursuant to the requirements of the Ohio Department of Administrative Services, Office of Information Technology (DAS OIT) State IT Standard ITS-SEC.02, which is 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 and NIST Special Publication 800-61 Revision 2, Computer Security Incident Handling.

III. APPLICABILITY

This policy applies to all Ohio Department of Rehabilitation and Correction (DRC) employees, contractors, volunteers, and other individuals who are authorized users of DRC system assets.

IV. DEFINITIONS

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.
- Attrition - An attack that employs brute force methods to compromise, degrade or destroy system assets or services, such as a DoS or a brute force attack against passwords, digital signatures or other authentication mechanisms.

- 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 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.

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 to and 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.

Denial of Service (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.
- Failed or successful attempts to cause failures in critical infrastructure services, loss of critical supervisory control and data acquisition services (SCADA).

Encryption - A technique that mathematically encodes your data before it is sent between your browser and the web site that you are currently visiting. Strong encryption makes it nearly impossible for anyone except the intended party to decode and obtain data transmitted to the intended party.

Improper Use/Access - The violation of acceptable computing laws, rules or policies which includes the suspected criminal use of system assets resulting in identity theft and/or the disclosure, improper access,

destruction or alteration of any state managed system asset or data. Improper usage or access includes potential violations of ORC Chapter 1347.

Information Spillage - Instances where sensitive information on a system asset is inadvertently exposed to unauthorized disclosure. Information spillage often occurs when information that is initially thought to be of lower sensitivity is transmitted to an information system and then is subsequently determined to be of higher sensitivity. Examples include:

- Sensitive information placed on information systems that are not authorized to process such information.
- Information thought to be public is posted on a state Web site but is later determined to contain non-public information.
- Non-public information added to a system asset which is not accredited to house non-public information.
- Misdirected e-mail or postal mail that contains sensitive information.

Information Technology (IT) Security Incident - A violation or imminent threat of violation of information system / computer security policies, acceptable use policies, or standard security practices that threatens the confidentiality, integrity or availability of any system asset. Computer security incidents include, but are not limited to:

- Unauthorized access to any system asset.
- Denial of service for any system asset.
- Installation of malicious code on any system asset.
- Improper usage or access of any system asset.
- Scans, probes and attempted access of any system asset.
- Information spillage for any system asset.
- Loss or theft of a DRC computing device or DRC media.
- The compromise, in any way, of any confidential, non-public and or Personally Identifiable Information (PII).

Loss or Theft - The loss or theft of a computing device or media used by a state agency, such as a laptop, smartphone, tablet, thumb/flash/jump drive/other media or authentication token or loss or theft of paper documents containing sensitive data or personally identifiable information (PII).

Malicious Code - Successful installation of malicious software (e.g., virus, worm, Trojan horse or other code-base malicious entity) that infects a system asset, typically an operating system or software application.

Personally Identifiable Information (PII) - Information that can be used directly or in combination with other information to identify a particular individual. PII includes:

- A name, identifying number, symbol or other identifier assigned to a person.
- Any information that describes anything about a person.
- Any information that indicates actions done by or to a person.
- Any information that indicates that a person possesses certain personal characteristics.

Recovery - Defined procedures or process within an information security incident response plan with the goal of returning the affected or compromised systems impacted by the violation or imminent threat of violation to normal operations, as well as confirming normal functionality and, if applicable, remediating known vulnerabilities to prevent future incidents.

Scans, Probes and Attempted Access - Any activity that seeks to access or identify a state computer, open ports, protocols, service or any combination on system assets for purposes of later attack or exploitation.

Sensitive Data - Any type of data that presents a high or medium degree of risk if released or disclosed without authorization. There is a high degree of risk when unauthorized release or disclosure is contrary to a legally mandated confidentiality requirement. There may be a medium risk and potentially a high risk in cases for which an agency has discretion under the law to release data, particularly when the release must be made only according to agency policy or procedure. The data may be certain types of PII that is also sensitive, such as medical information, social security numbers and financial account numbers. In addition, the data may be other types of information not associated with a particular individual such as security and infrastructure records, system administrative passwords, trade secrets and business bank account information.

SQL Injection - A code injection attack initiated to exploit a given database security vulnerability. A SQL injection can allow attackers to spoof identity, tamper with existing data through disclosure, destruction or inaccessibility or permit the attacker to become an administrator on the database server.

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 and therefore, must be protected by the appropriate security requirements to ensure business continuity.

Unauthorized Access - An attempt to gain unapproved logical or physical access to a DRC system asset or a change to an information technology system, firmware, hardware or software configuration characteristics without the state's knowledge, instruction or consent.

V. POLICY

It is the policy of the Ohio Department of Rehabilitation and Correction (DRC) to utilize a DRC IT security incident response team and standardized procedures for responding to IT security incidents in order to protect DRC system assets pursuant to the requirements of the Ohio DAS OIT State IT Standard ITS-SEC.02, which is 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 and NIST Special Publication 800-61 Revision 2, Computer Security Incident Handling.

VI. PROCEDURES

- A. DRC shall maintain an IT security incident response team, which shall be comprised of the following representatives:
 1. The Chief of BITS, who shall co-chair the team;

2. The CISO, who shall co-chair the team;
 3. Staff members from BITS and additional authorized users at the technical, selected by the Chief of BITS;
 4. A representative from the Legal Services Division, selected by the Chief Legal Counsel;
 5. A representative from the Chief Inspector's Office, selected by the Chief Inspector;
 6. A procurement representative from the Office of Administration, selected by the Deputy Director of the Office of Administration;
 7. A representative from the Bureau of Communication, selected by the Director; and
 8. Representatives from the impacted data owners, when the team is activated to respond to a DRC IT security incident.
- B. The DRC IT security incident response team shall be responsible for:
1. Conducting or recommending training for:
 - a. DRC authorized users at the technical level. Training may include a review of the DAS OIT enterprise IT security incident response plan and required DAS OIT and DRC incident response processes and procedures.
 - b. DRC authorized users at the end user level. Training may include an overview of the DRC IT security incident response process and procedures and steps that end users can take to protect against common attack vectors.
 2. Maintaining a current list of all authorized users at the technical level in BITS and in facilities/regions that may be called upon to respond when a DRC IT security incident occurs or is threatened. The list shall include business and personal contact information and a summary of the users' technical training, expertise and skills.
 3. Providing guidance to authorized users at the technical level in BITS and in facilities/regions to assist them in performing the appropriate duties, tasks and activities necessary to support DRC IT security incident assessment, evaluation, analysis, response and follow-up.
 4. Participating in DAS OIT incident response exercises and conducting DRC incident response exercises.
 5. Responding in a timely, efficient, and effective manner when a DRC IT security incidents occurs or is threatened, to properly identify, assess, evaluate, report, contain and eradicate/remediate the incident in order to ensure a successful recovery and protect DRC system assets.

6. 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.
- C. DRC authorized users at the technical level assigned to BITS and to DRC facilities/regions shall perform the appropriate duties, tasks, and activities, as directed by DAS OIT, the Chief of BITS and the CISO, to support DRC IT security incident assessment, evaluation, analysis, response and follow-up. These duties, tasks, and activities may include, but are not limited to:
1. Profiling DRC networks and systems in order to measure the characteristics of expected activity so that changes can be more easily identified;
 2. Studying DRC networks, systems and applications, by conducting frequent log reviews in order to understand their normal functionality so that abnormal functionality can be more easily recognized and understood;
 3. Following recommended retention policies for logs recorded in a variety of key areas, such as firewalls, intrusion detection/prevention systems (IDS/IPS) and core business applications, such as DOTS portal and OnBase;
 4. Performing incident correlation by reviewing multiple indicator sources for incident precursors, such as firewall, server, security and intrusion detection sensor logs;
 5. Keeping all host clocks synchronized with a network time protocol source to ensure consistent timestamps in all logs;
 6. Maintaining a centralized security incident knowledge source that can be referenced quickly for all DRC authorized users at the technical level, especially the users that will be tasked to respond to a DRC IT security incident;
 7. Using Internet search engines on computing devices segregated from the DRC network to research information about unusual activity and attack vectors;
 8. Running packet sniffers when an IT security incident appears to be occurring over a DRC network to capture and record network traffic for analysis;
 9. Utilizing appropriate software tools and human analysis filters to filter out indicators that tend to be insignificant, such as malicious logic that is successfully quarantined by antivirus software or that falls within normal or expected behaviors; and
 10. Attending training and incident response exercises to improve their proficiency in assessing, evaluating, analyzing, and responding to IT security incidents.
- D. All DRC authorized users shall report any known, suspected or threatened IT security incidents by completing the following two (2) required reports:
1. A ticket in ServiceNow, pursuant to DRC Policy 05-OIT-25, Standardized DRC IT Reporting and Requesting Procedures; and

2. An Incident Report (DRC1000), pursuant to the requirements of DRC Policy 01-COM-08, Incident reporting and notification.
- E. When the Chief of BITS or CISO is informed ~~that~~ a DRC IT security incident has occurred or is threatened, the Chief of BITS or CISO shall:
1. Obtain the necessary additional information and evidence about the incident from the reporting parties and/or the impacted data owners, which shall include:
 - a. Data and time detected;
 - b. Date and time occurred;
 - c. A description of the current status; and
 - d. A description of the incident and its impact on DRC system assets, users and/or data owners.
 2. Notify the Director/designees and other administrators, as appropriate, about the incident and, if warranted by the nature and severity of the incident, consult with the Chief Legal Counsel and/or Chief Inspector to determine if the Ohio State Highway Patrol should be notified of possible criminal behavior.
 3. Assess and evaluate the scope and severity of the incident and prioritize the incident based on the following factors:
 - a. The immediate functional impact on DRC business operations and the likely future functional impact on DRC business operations if the incident is not immediately contained;
 - b. The type and extent of DRC information impacted (e.g. sensitive data, PII, etc.);
 - c. The amount of time, effort and resources needed to successfully achieve recovery; and
 - d. Whether the incident rises to the level that necessitates the activation of critical incident management procedures, as detailed in DRC policy 310-SEC-14, Critical Incident Management.
 4. Identify the probable level of resources necessary to contain and eradicate/remediate the incident and request assistance and resources from DAS OIT, if it is determined that the DRC IT security incident response team lacks sufficient resources to respond to the incident.
 5. If warranted by the nature and severity of the incident, open a formal, written log to document all steps taken in response to the incident.

6. If warranted by the nature and severity of the incident, establish a formal incident command center with appropriate telecommunication and IT access.
 7. Report the incident by telephone or e-mail to the DAS OIT Customer Service Center (CSC). The report shall include:
 - a. Date and time detected;
 - b. Date and time occurred;
 - c. A description of the current status;
 - d. A description of the incident and its impact on DRC system assets, users and/or data owners;
 - e. A list of external organizations impacted by the incident;
 - f. A description of the source or cause and a description of previous incident occurrences, if known;
 - g. A description of actions taken, thus far, to respond to the incident;
 - h. A description of the projected level of resources, time, and effort necessary to quickly contain and eradicate/remediate the incident, including a request for assistance and resources from DAS OIT, if it is determined that the DRC IT security incident response team lacks sufficient resources to respond to the incident; and
 - i. A list of key DRC staff members leading the response and the contact information for said staff members.
 8. As a follow-up to the report submitted to the DAS OIT CSC, report the incident to:
 - a. DRC users impacted by the incident;
 - b. External organizations impacted by the incident; and
 - c. The appropriate DAS OIT administrators, if warranted by the nature and severity of the incident.
 9. Activate the DRC IT security incident response team and notify authorized users at the technical level, DAS OIT and others that may be called upon to assist in responding to the incident.
- F. All resources activated to respond to the incident, including the DRC IT security incident response team, authorized users at the technical level from BITS and DRC facilities/regions, DAS OIT and any others mobilized for the effort, shall:

1. Identify the appropriate containment strategy and define acceptable risks in implementing the strategy, with the ultimate goal of minimizing the damage to DRC system assets in the most expedient manner. Criteria for identifying the appropriate incident containment strategy include, but are not limited to:
 - a. The type and nature of the presenting attack vector(s);
 - b. The potential damage to data or theft of data;
 - c. The impacted hosts that require remediation;
 - d. The need for evidence preservation;
 - e. Services availability to impacted internal and external users;
 - f. The overall time, effort and resources necessary to implement the containment strategy in order to effect a successful recovery solution;
 - g. The effectiveness of the containment strategy (i.e., partial containment, full containment); and
 - h. The estimated time from implementation of the containment strategy to eradication/remediation and recovery.
 2. Take the necessary steps to implement the containment strategy and eradicate/remediate the damage caused during the course of the incident in order to achieve recovery. During recovery:
 - a. The impacted system assets ~~will~~ shall be restored to normal operation and functionality;
 - b. Normal operation and functionality of the impacted system assets ~~will~~ shall be confirmed, preferably by a group of users directly impacted by the incident;
 - c. If applicable, vulnerabilities identified during the course of responding to the incident shall be remediated to prevent future similar incident occurrences.
 3. Keep all necessary parties (i.e., Director, impacted internal and external users, DAS OIT) advised of the status and progress of the containment, eradication/remediation at designated intervals until the incident is concluded and recovery is achieved.
- G. At the conclusion of the incident, when recovery is achieved, the Chief of BITS or CISO shall:
1. Conduct an informal closing debriefing session with the responders, including the DRC IT security incident response team, authorized users at the technical level from BITS and DRC facilities/regions, DAS OIT and any others mobilized for the effort to review the response to the incident.

2. Complete a written after action report, which shall serve as the formal documentation of the incident response. The report shall be distributed to the Director, the appropriate DRC administrators, DAS OIT, and other applicable individuals and, at a minimum, shall include:
 - a. A description of the root cause of the incident and the incident's impact;
 - b. A chronology, from initial discovery of the incident to recovery, of all actions taken, the times the actions were taken and the names of the responders performing the actions to contain and eradicate/remediate the incident; and
 - c. Recommendations to reduce future vulnerabilities and similar incident occurrences and recommendations to improve the level of incident response.
- H. After completion of the debriefing session and written after action report, the Chief of BITS or CISO shall conduct a formal lessons learned meeting with the DRC IT security incident response team, other responders, data owners, users, etc. For major incidents, the lessons learned meeting should be conducted as soon as possible after recovery from the incident. For lesser incidents, the lessons learned meeting ~~can~~ may be conducted during a regularly scheduled meeting of the DRC IT security incident response team.
 1. During the lessons learned meeting, the following topics should be addressed:
 - a. Updates about the root cause of the incident, the incident's impact and the status of recovery;
 - b. Analysis of incident characteristics to identify systemic security vulnerabilities, gaps and threats and additional risk assessment procedures or security controls required to address future incident occurrences; and
 - c. Analysis of the incident response to identify ways in which incident response can be improved.
- I. At the statewide level, DAS OIT supports state agency IT security incident response efforts by providing the following resources:
 1. An enterprise IT security incident response tracking system to collect pertinent information about IT security incidents;
 2. A list of recommended software and hardware for analysis of IT security incidents (e.g., digital forensic workstations, servers, networking equipment or virtualized equivalents; packet sniffers, removable media, etc.);
 3. An enterprise IT security incident response plan that serves as a plan template for state agencies and contains the following components:
 - a. The organization and structure of the enterprise response capability.

- b. DAS OIT and state agency incident response contact information, roles and responsibilities.
 - c. Protocols for communication during the incident response.
 - d. Guidance for incident assessment and evaluation (i.e., collection, analysis, classification, forensic/evidentiary considerations, etc.).
 - e. Best practices for incident containment, eradication, recovery and reporting.
 - f. Reporting and metrics;
4. An enterprise IT security incident response team responsible for:
 - a. Conducting training for state agencies that may include a review of the enterprise IT security incident response plan and required incident response processes and procedures.
 - b. Leading incident response exercises.
 - c. Engaging in proper incident monitoring, assessment, evaluation, containment, eradication, recovery and follow-up.
 - d. When IT security incidents occur, coordinating with individual state agency security points of contact and individual state agency IT security incident response teams to ensure that the incidents are properly identified, contained and eradicated/remediated and to assist in recovery efforts.
 - e. Providing guidance on how to detect and analyze incidents that use common attack vectors;
5. Procedures for analyzing IT security incident precursors and indicators at both the enterprise and agency level;
6. Basic and advanced IT security incident response training to support individual agency security incident response procedures; and
7. Annual IT security incident response testing exercises, utilizing automated tools as much as practical, which simulate security incidents and allow individual agencies to measure the effectiveness of their response capability and identify response strengths and potential weaknesses.