admin
THE SOUTH CAROLINA
DEPARTMENT of ADMINISTRATION

SCDIS-201 Information Security and Privacy Incident Response Standards

For South Carolina State Agencies
Version 1.0
Issued: October 7, 2016
Effective: July 1, 2016

Purpose

These standards define the requirements for response by State of South Carolina (State) agencies to information security and privacy incidents. These standards are compliant with the *SCDIS Information Security Program Master Policy* and are consistent with the requirements in *SCDIS-200 Information Security and Privacy Standards*, (http://www.admin.sc.gov/technology/information-security/policies-and-procedures).

Scope

Pursuant to Proviso 93.25 of the 2016–2017 South Carolina Appropriations Act and any successive statutes, these standards are to be implemented by State agencies, including institutions, departments, divisions, boards, commissions and authorities. Exceptions are noted in the terms of the Proviso.

Within statutory scope, these standards apply to:

1. All persons managed by an agency, such as employees, contractors and volunteers;
2. All agency information systems, regardless of location or service level agreement; and
3. All information, regardless of media.

Definitions

Within the scope of this document, the following terms are used as defined here:

Agency – Refers to State agencies, including institutions, departments, divisions, boards, commissions and authorities.

Incident – An event or series of related events that pose a threat to the confidentiality, integrity, or availability of information or information systems. These events violate security and/or privacy policy. Examples: intrusion or infection of a computer device; lost computer; lost paper or digital media; and misdirected email or fax.

Privacy Breach – A type of incident which includes the access, use, disclosure and/or distribution of sensitive information in violation of a law or regulation.

Sensitive Data – Refers to information that is protected against unwarranted disclosure, whether by law, regulation, and/or policy.

Unauthorized Access: When an investigation of a CSIR Tier 2A, CSIR Tier 2B or Non-CSIR incident determines that access to data without an approved business need has likely occurred.

Roles

Agency Computer Forensics Investigator – An individual in a state agency who has been nominated by the agency director and approved by DIS to perform computer forensics investigations for their agency. The approved investigator will possess experience and expertise in computer forensics in accordance with industry best practices, will be familiar with the DIS SOC process and reporting requirements, and validated annually.

Agency Privacy Liaison – The individual or their designee who is responsible for ensuring agency compliance with the State privacy policies.

Agency Security Liaison – The individual or their designee who is responsible for addressing information security issues.

Division of Information Security (DIS) – An operating unit under the South Carolina Department of Administration (Admin), responsible for a variety of statewide policies, standards, programs, and services relating to cybersecurity and information systems.

Division of Technology Operations (DTO) Service Desk –An operating unit under Admin's DTO serving as a single point of contact for Admin's customers who need assistance with IT services. The Division of Technology Operations Service Desk will assist with the tracking and management of incidents.

Enterprise Privacy Office (EPO) – An operating unit under Admin, responsible for advising State agencies on the management of personal information as well as establishing, assessing and enhancing privacy protection policy, training and compliance measures.

Security Operations Center (SOC) – A unit under the DIS responsible for ensuring information systems are sufficiently monitored to detect attacks and/or signs of potential attacks, including unauthorized network local or remote connections**.**

Guiding Principles

These guiding principles should be used to assist in the interpretation of the intent of all directives within this document, and to assist in the review, modification and addition to these directives.

1. **Executive Leadership Must Provide Resources and Support for the Incident Response Plan** – Agency executives must assign responsibility, prioritize efforts and authorize resources needed for the development, implementation, operation and maintenance of the agency's incident response plan.
2. **Incident Response is Everyone's Responsibility** – All agency personnel are responsible and accountable for:
   - Understanding their responsibilities within the context of an information security or privacy incident.
   - Reporting suspected and actual information security or privacy incidents to designated information security and privacy personnel.
   - Cooperating with designated information security and privacy personnel in performance of the incident response process.

Components of an Incident Response Program

Each agency must develop and implement its incident response program to ensure that information security and privacy incidents occurring within the agency are appropriately reported and handled. Below are the core components of an incident response program.

1. **Incident Response Plan**
   Each agency must develop, document and internally publish an incident response plan that should at a minimum:
   - Define resources, such as technology and personnel, required to effectively support incident response capabilities.
   - Develop procedures for implementation of the incident response program, consistent with the SCDIS-201 Information Security and Privacy Incident Response Standards.

- Determine the tools and technologies to be utilized in detection of information security and privacy incidents.
- Implement a robust training plan to promote awareness among agency workforce of the requirement to identify and report incidents.
- Establish metrics to ensure incident response capabilities remain effective.
- Require the review and update of the incident response plan on an annual basis.

2. **Information System Monitoring**
   - Each agency must ensure that information systems are sufficiently monitored to detect attacks and/or signs of potential attacks, including unauthorized network, local or remote connections. Agencies must be monitored by the DIS SOC to certain baseline levels. Refer to SCDIS-210 *InfoSec Technology Coverage Standards* for monitoring levels in use by the DIS SOC.
   - Each agency must ensure that monitoring devices are deployed strategically within the information technology environment to collect information security events and associated information.
   - Each agency must ensure information obtained from information security and privacy monitoring tools is protected from unauthorized access, modification and deletion.
   - Each agency must ensure the monitoring of inbound and outbound communications traffic of information systems for unusual or unauthorized activities or conditions.

3. **Incident Reporting**
   - Agencies retain the primary responsibility and accountability for ensuring that responses to information security and privacy incidents comply with federal and state laws and regulations.
   - Each agency must ensure that personnel are required to report suspected and actual information security and privacy incidents to the agency security or privacy liaison.
   - Agencies shall inform Admin of information security incidents which present suspected or actual risk to sensitive data, and any suspected or actual privacy breaches, within 24 hours of discovery. Agencies shall designate a point of contact for reporting such incidents to Admin, and the agency will incorporate these reporting requirements into their Agency incident response procedures. (This function may fall within the duties of the privacy or security liaison.)

4. **Incident Handling**
   - Each agency must ensure that information security and privacy incident handling processes include preparation, detection and analysis, containment, eradication and recovery.
   - Each agency must ensure the implementation of incident response tools such as intrusion detection, firewalls and incident investigation tools, to effectively respond to security or privacy incidents.
   - Agencies wishing to perform their own computer incident forensics/technical investigations must submit a letter to DIS describing their incident response and forensics investigation procedures, including how those procedures interact with the DIS SOC processes, and certifications of designated agency computer forensics investigators. Before any agency can begin performing computer incident investigations, DIS must approve an agency's incident response procedure and of each agency investigator.

5. Incident Response Training
   - Each agency must provide training that includes incident recognition and reporting procedures to all agency personnel within one month of hire, and annually thereafter.
   - Each agency must provide incident response training within one month of personnel assuming incident response roles or responsibilities, and annually thereafter.
   - Each agency must provide training to incident response personnel upon significant changes to information systems and/or changes to the incident response plan.

6. **Incident Response Testing**
   - Each agency must establish a formal process to test incident response capabilities, and conduct testing on an annual basis to determine the incident response effectiveness and adequacy.
   - Each agency must document the incident response test results and update incident response processes as applicable.

7. **Malicious Code Protection**
   - Each agency must ensure malicious code protection mechanisms are employed for information systems, to detect and eradicate malicious code.
   - Each agency must ensure malicious code protection mechanisms are updated whenever new releases are available.
   - Each agency must ensure malicious code protection mechanisms are configured to perform periodic scans at defined time intervals.
   - Each agency must ensure malicious code protection mechanisms are configured to send an alert to inform appropriate personnel to initiate appropriate actions in response to malicious code detection.

Incident Response Types and Tier Levels

At the time an information security or privacy incident is reported, the incident is assigned a type, Computer Security Incident Response (CSIR) or Non-Computer Security Incident Response (Non-CSIR). CSIR's are also assigned a tier level. The type of incident determines the incident handling process. The tier level describes the level of risk to sensitive data. The tier level of an incident may change as additional information is discovered during the investigation process.

Below is a description of the types and tier levels used during the incident handling process.

Computer Security Incident Response (CSIR) – The process used for incidents that generally involve intrusion or infection of a computer device and that are handled by the Security Operations Center in collaboration with the Enterprise Privacy Office and agency privacy and security liaisons. Please see the following descriptions of CSIR tier levels.

CSIR Tier 1: These incidents originate from law enforcement actions. Examples: warrant for seizure of a computer; law enforcement evidence request.

CSIR Tier 2A: Incidents where there is a potential for restricted data to be affected.

CSIR Tier 2B: Incidents where there is potential for confidential or other sensitive data to be affected.

CSIR Tier 3: These incidents involve a suspected or confirmed compromise of a computing device by malware or cyber intrusion in such a way that data may be tampered or exfiltrated. Tier 3 is a temporary assignment. Tier 3 incidents are reassigned an alternate tier level after further investigation of the incident. Examples: malware designed to capture credentials; malware designed to encrypt or delete data; and hacker access to a server.

CSIR Tier 4: Incidents where there is no potential for confidential or restricted data to be affected.

CSIR Tier 5: These incidents may involve suspected or confirmed compromise of a computing device by malware or cyber intrusion in such a way that data may not be tampered or exfiltrated. These incidents may also affect availability of information systems or the exposure of potential vulnerabilities. Examples: advertising malware; click-fraud malware; and browser toolbar malware.

Non-Computer Security Incident Response (Non-CSIR): The process used for incidents that do not involve intrusion or infection of a computing device, but still have potential to involve the loss or unauthorized access of sensitive data. These incidents are handled by the agency privacy liaison in collaboration with the Enterprise Privacy Office, as needed. Examples: lost computer; lost paper or digital media; and misdirected email or fax.

Incident Response Steps

For the sake of efficiency, these steps may be performed in series or concurrently. **Coordination between the agency, the Division of Information Security, and the Enterprise Privacy Office must be maintained**.

For All incidents

1. **Preparation**. Prepare your incident response plan in advance of execution.
   1.1. Assign responsibilities to appropriate staff members.
   1.2. Train all staff members in the incident response process.
   1.3. Obtain any technical resources needed to perform incident response.

For CSIR Incidents

2. **Incident Reporting.** An incident can be detected by the SOC, the agency, a citizen or others.
   2.1. **When the SOC detects a computer security incident or state agencies detect a computer security incident that poses a potential or actual risk to sensitive data**, the incident will be reported to the SOC, entered into the SOC Incident Response Tracker System, **assigned as type CSIR** and **classified with an initial tier level** (refer to Incident Response Types and Tier Levels for definition). The agency privacy and security liaisons and others, as identified by the agency, will then receive notification of any Tier 2-5 incidents.
   2.2. **When entities other than the SOC or state agencies, detect an incident**, the incident will be reported to the SOC or the DTO Service Desk. The type of incident will be **assigned as type CSIR** and the SOC will be notified of the incident. The incident will be entered into the SOC Incident Response Tracker System, and **classified with an initial tier level**. The agency privacy and security liaisons and others as identified by the agency will then receive notification email for any Tier 2-5 incidents.
   2.3. Within one hour of incident notification, the agency must acknowledge receipt of the notification by replying to the notification email.
3. **Classification.** The initial tier level assigned by the SOC, determines the subsequent handling process for the incident.
   3.1. **Tier 1 Incidents** – Tier 1 incidents are handled internally, including only those participants identified by General Counsel. Additional personnel will be involved only as needed for the investigation.

   3.2. **Tier 3 Incidents** – Classification as a Tier 3 is temporary. Tier 3 incidents will be reclassified to Tier 2, 4, or 5 depending on whether sensitive data may be involved.
      3.2.1. Within 24 hours of a Tier 3 incident notification, the agency privacy liaison will provide to the SOC the classification level of the data potentially involved in the incident, as defined by the State of South Carolina Data Classification Schema, identifying whether the incident potentially involves sensitive data. If there is potential sensitive data involvement, the incident will then be reclassified as Tier 2.
      3.2.2. Tier 3 incidents where there is no potential for sensitive data to be affected are reclassified as Tier 4 or 5.

   3.3. **Tier 2 Incidents** – If it is determined by the agency privacy liaison that the incident potentially involves unauthorized access to <u>confidential</u> data, the incident is reclassified as a Tier 2B. If the incident potentially involves access to <u>restricted</u> data, the incident is reclassified as Tier 2A. At the discretion of the agency privacy liaison in consultation with the EPO, an incident involving

Internal Use data may also be classified as Tier 2A or 2B. The SOC or an authorized agency investigator initiates a technical investigation using the following steps.

3.3.1. **Identification** – Confirm the technical details of the incident.

IMPORTANT: These steps must only be performed by qualified incident investigators, using an incident response procedure approved by the Division of Information Security. (Refer to Incident Handling paragraph in Components of an Incident Response Program section above.)

3.3.1.1. **Preserve Evidence** – Using a forensically sound method, record network and host-based information related to the incident.

IMPORTANT: Do not run antivirus scans or other file system diagnostic tools on the original hard drive(s). Such actions can affect file system timestamps, hindering or invalidating a subsequent technical investigation.

3.3.1.1.1. Document the system's internal time, and its skew from real time. Also document the system's configured time zone and daylight time observed setting.

3.3.1.1.2. Using an incident response data collection tool, collect memory and file system artifacts. If such a tool is not installed, collect binary images and hashes of all hard drives.

3.3.1.1.3. Shut down the system and remove all internal and attached hard drives. Observe chain-of-custody rules and documentation for these hard drives.

3.3.1.2. **Confirm Incident** – Using collected incident response data or hard drive image(s), confirm corroborating evidence of the original indicators of compromise. Using SIEM, IDS or similar technology, collect network-based security events related to the incident. If strong evidence exists to explain all indicators of compromise as being false, the incident may be closed as a false positive and the original hard drives returned to service. Otherwise, proceed with the following steps.

3.3.1.3. **Construct Timeline** – Construct a timeline correlating all relevant network-based and host-based incident data, correcting data timestamps as appropriate for documented system time skew, time zone and daylight savings time changes.

3.3.1.4. **Compare Indicators of Compromise** – Match the indicators of compromise against the timeline. Document causes.

3.3.1.5. **Identify Malicious Intrusion** – Identify additional indicators of malicious intrusion, such as malware, misconfiguration, or vulnerability.

3.3.1.6. **Determine Degree of Compromise** – Determine the likelihood of sensitive data compromise. **If evidence indicates a malicious intrusion has the capability and opportunity to compromise sensitive data, the potential for sensitive data compromise must be reported as a finding, to include an estimation of likelihood based on available evidence, observations or information. Report any such finding to the agency privacy liaison without delay.**

3.3.1.7. **Provide the investigation report to the SOC.**

3.3.1.8. At the conclusion of the investigation, **promptly report the incident and all details to the agency privacy liaison.**

3.3.2. **Containment** – Disable, remove or otherwise stop the local source of the incident from further compromise.

3.3.2.1. If evidence from the investigation indicates a possibility of related compromise of other systems, take appropriate steps to prevent or contain and investigate those.

3.3.2.2. If evidence from the investigation indicates unauthorized access of sensitive data, promptly notify incident response personnel by sending a reply to the SOC incident notification email.

3.4. **Tier 4 or 5 Incidents** – The SOC will provide recommended eradication and recovery processes to agency IT Support Services.

3.5. **Eradication** – Remove the source of the compromise if it is still a threat.

3.6. **Recovery** – Return the system to service with replacement hard drive(s) installed.

3.7. **Post Incident Review** – For Tier 2 incidents, take corrective actions to improve processes or technologies as investigation findings indicate.

For Non-CSIR Incidents

2. **Incident Reporting.** An incident can be detected by the agency, a citizen or others. Agencies shall identify an appropriate entity to be notified. (This notification could be made by way of a service desk or directly to the security or privacy liaison or another designee.) The incident is designated **as type Non-CSIR** (refer to Definitions).

2.1.1. **Notification** –In the event that an incident is a suspected or actual privacy breach, the designated agency point of contact will report it to the EPO. The EPO will collaborate with the agency, as needed, during the incident handling process.

3. **Incident Handling**. The agency ensures that the following handling process will be followed:

3.1. **If a computer device, including laptop and personal storage devices, was lost or stolen:**

3.1.1. **Determine if the data on the device is accessible** – Agency IT Support Services should determine if the device was properly secured. If encryption was in place and data was inaccessible, the agency closes the investigation pending any special notification requirements.

3.2. **If the device was not secured and data was accessible, or sensitive data in paper or digital media, email or fax was at risk:**

3.2.1. **Identification** – The agency privacy liaison confirms the details of the incident.

3.2.2. **Preserve Evidence** – The agency privacy liaison reviews a copy of the information that was disclosed or accessed, or makes a list of any information that was disclosed or accessed inappropriately.

3.2.3. **Determine Immediate Mitigation Actions –** The agency performs immediate mitigation of the unauthorized access or disclosure, as directed by the agency privacy liaison. Some actions may include:

3.2.3.1. Retrieve the data and/or device from the recipient, if possible.

3.2.3.2. If recipient is known, obtain written agreement from the recipient that the information will not be further disclosed.

3.2.3.3. Complete a remote wipe of the device, if appropriate.

3.2.4. **Construct Timeline** – Construct a timeline correlating all relevant details about the incident.

3.2.5. **Conduct Investigation and Document Risk Assessment-**Document investigation findings. Assess risks to the individual and organization resulting from the incident. Determine statutory, regulatory or policy requirements such as reporting and notification.

3.2.6. **Finalize Mitigation Plan** –

3.2.6.1. Additional mitigation actions may be identified and completed.

3.2.6.2. Complete notifications, as required.

3.2.6.3. Identify and apply safeguards.

3.2.7. **Post Incident Review** – Based on investigation findings, take corrective actions to improve processes or technologies as appropriate.

Guidance

The Division of Information Security and Enterprise Privacy Office shall provide guidelines, document templates, tutorials or other forms of assistance for the use of Agencies by distribution means appropriate to the nature and sensitivity of the content, upon request.