SCDIS-301 Information Security and Privacy Incident Response Plan Development Guidelines

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

Purpose

This document provides guidance to State of South Carolina (state) agencies in developing agency Incident Response Plans. An Incident Response Plan is a collection of documents demonstrating compliance with the incident response requirements within the South Carolina Information Security Program (refer to *SCDIS-200 Information Security and Privacy Standards* and SCDIS-201 Information Security and Privacy Incident Response Standards, http://admin.sc.gov/technology/information-security/incident-response).

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.

Executive Roles and Responsibilities

The executive director of an agency plays a vital role in the development of the agency's Incident Response Plan, empowering staff with the authority to act decisively, and providing the resources necessary to design and implement the plan.

The agency executive director should:

1. Communicate to the agency's senior management the agency's commitment to, and priority for development of its Incident Response Plan.
2. Review the steps outlined in the Management Roles and Responsibilities below, then designate and charge appropriate members of senior management with the responsibility and authority to perform those steps.
3. Require periodic progress reports on the development of the agency's Incident Response Plan.

Management Roles and Responsibilities

Agency management should ensure that agency staff follow the processes outlined in this document, report progress to executive leadership, and provide or escalate resource needs.

Management should also:

1. Review the Technical Roles and Responsibilities below, as well as the Roles and Responsibilities Chart template published on the DIS webpage: http://www.admin.sc.gov/technology/information-security/resources
2. Designate and charge appropriate staff members with the responsibility and authority to perform the associated tasks.
3. Require staff members to complete incident response training when hired and annually.
4. Require periodic progress reports on the task assignments.

Technical Roles and Responsibilities

The **security and privacy liaisons** are the lead staff members charged with coordinating the processes outlined below. The security and privacy liaisons should have project management skills in order to organize and manage actions of the staff members who compose the incident response team.

The security and privacy liaisons should

1. Review and become familiar with the requirements specified in *SCDIS-201 Information Security and Privacy Incident Response Standards*.
2. Compare the standards to existing agency processes and documentation, and perform a gap analysis to determine needed remediation.
3. Develop or revise the agency's incident response procedures to describe in detail the processes it will follow for each of the incident types identified in *SCDIS-201 Information Security and Privacy Incident Response Standards,* as well as define responsibilities for initiation and execution of these processes.
4. Create and maintain the agency Incident Response Plan master document, including the following elements:
   - A reference to the State Incident Response Plan, including URL (http://www.admin.sc.gov/technology/information-security/incident-response)
   - A list of all documents created in the procedures above, including location(s) where master copies are kept.
   - A list of all relevant agency policies, procedures and other documents that were reviewed, modified or created during the procedures above, including location(s) where master copies are kept.

- Ensure that all document products of this process are secured in such a way that they are only accessible to the appropriate agency staff members.

5. Ensure incident responders have appropriate tools and training to perform their roles within incident response processes.
6. Ensure all agency staff understand their responsibilities for recognizing and reporting incidents and/or privacy breaches.