

Idaho Technology Authority (ITA)

ENTERPRISE STANDARDS – S6000 SECURITY

Category: S6010 – CYBERSECURITY INCIDENT AND BREACH RESPONSE MANAGEMENT AND REPORTING

CONTENTS:

- I. [Definitions](#)
- II. [Rationale](#)
- III. [Incident and Breach Response Roles and Contact Information](#)
- IV. [Approved Standard\(s\)](#)
- V. [Reference Documents](#)
- VI. [Contact Information](#)
- VII. [Review Cycle](#)
- VIII. [Revision History](#)

I. DEFINITIONS

Vocabulary for Event Recording and Incident Sharing (VERIS): A taxonomy and a set of metrics designed to:

1. Provide a common language in the enterprise for describing security incidents in a structured and repeatable manner
2. Provide a foundation from which the enterprise can constructively and cooperatively learn from agencies to better measure and manage risk
3. Provide metrics for risk management and IT investment

II. RATIONALE

When public trust, reputation, and costs are at stake, it is critical that agencies identify and respond to incidents and breaches in a consistent, repeatable, and cost-effective manner. An incident response capability within an agency is a complex activity and it is important to develop an overarching program that identifies the key processes for incident response governance. It is equally important for incident and breach investigation information to be documented based on a common language for benefits such as intelligence sharing, risk management, metrics, and decision-making.

III. INCIDENT AND BREACH RESPONSE ROLES AND CONTACT INFORMATION

NOTE: To report an incident or breach, agencies can refer to ITA Enterprise Guideline G585 (Cybersecurity Incident and Breach Response) to align and establish their procedures. The following roles and contact information are for quick reference.

Entity	Role	Phone Number	Email Address
Information Technology Services (ITS)	<ul style="list-style-type: none"> Assist with incident response and management Escalates incidents to Risk Management if a breach is determined Oversees the ITS incident response governance program 	Incident Response Line 208-605-4000	cyberrisk@its.idaho.gov
Office of Risk Management	<ul style="list-style-type: none"> Provides breach management services to assist agencies Provides access to State cyber insurance coverage Provides professional breach management and legal support. 	Risk Management Line 208-332-1869	
Office of the Attorney General (AG)	<ul style="list-style-type: none"> Provides agencies legal advice in the event of a breach Coordinates efforts with the Office of Risk Management 	Contact your Agency Deputy Attorney General (DAG)	Contact your Agency Deputy Attorney General (DAG)

IV. APPROVED STANDARD(S)

A. NIST SP 800-53 Incident Response Family of Controls (IR-1 – IR-8)

All agencies will implement NIST SP 800-53 Incident Response family of controls (IR-1 through IR-8) within their agency. Agencies shall use a minimum impact level of moderate (MOD).

NIST SP 800-53 Family of Controls (IR-1 – IR-8)	
Control #	Standard
Global	<p>The enterprise incident response capability will work in a distributed model team structure.</p> <p>References: NIST SP 800-61</p>
IR-1 Incident Response Policy and Procedures	Agency will develop, document, and disseminate incident response related policies and procedures to its end-users and incident response personnel within its organization.

	<p>Agency will review, and revise if necessary, incident response policies and procedures <i>at least annually</i>.</p> <p>References: NIST SP 800-12, 800-61, 800-83, 800-100</p>
IR-2 Incident Response Training	<p>Agency will provide incident response training to its end users and incident response handlers <i>at least annually</i> or when needed (such as for information system changes, after an incident or breach, or from a threat/vulnerability assessment, etc.)</p> <p>References: NIST SP 800-16, 800-50</p>
IR-3 Incident Response Testing	<p>Agency will test the incident response capability for its organization <i>at least annually</i>.</p> <p>References: NIST SP 800-84, 800-115</p>
IR-4 Incident Response Handling	<p>Agency will approach incident handling for both incidents and breaches based on best practices which considers preparation, detection and analysis, containment, eradication, and recovery phases.</p> <p>Note: ITS will be responsible for incident response handling for ITS customers.</p> <p>References: NIST SP 800-61</p>
IR-5 Incident Response Monitoring	<p>Agency will investigate, track, and document incidents and breaches for the purposes of reporting the incident, generating metrics for analysis, threat and vulnerability modeling, improving defense-in-depth strategies, risk management analysis, etc.</p> <p>Agencies will document incidents and breaches using the VERIS Investigation Report Form. This establishes a common language for documenting incident/breach events throughout the enterprise.</p> <p>Note: ITS will be responsible for incident response monitoring for ITS customers.</p> <p>References: NIST SP 800-61</p>
IR-6 Incident Response Reporting	<p>Agency will establish timely reporting requirements for its end users. Agency will also establish timely reporting requirements to enterprise stakeholders as follows:</p>

	<p>1. <u>Incidents</u>: Within five (5) business days of discovery, agency will report incidents to ITS. Initial report will be a best effort with information currently available, pending a full investigation. Weekly status reports will be submitted to ITS. A full investigation report must be provided within 30-days.</p> <p><u>Note</u>: If a full investigation requires more than 30-days, contact ITS.</p> <p>2. <u>Breaches</u>: Within 24 hours to ITS, Office of Risk Management (ORM), and the Attorney General's Office</p> <p>Agency can refer to ITA Enterprise Guideline G585 (Incident and Breach Reporting) to align and establish their reporting procedures.</p> <p>Agency will use the electronic incident response report form to report incidents. In the event the electronic incident response form is unavailable submit the VERIS investigation report form to cyberrisk@its.idaho.gov.</p> <p>Note: ITS will be responsible for incident response reporting for ITS customers.</p> <p>References: NIST SP 800-84, 800-115</p>
IR-7 Incident Response Assistance	<p>Agency will discuss available services with ITS if the agency suspects or determines that a breach of information has occurred.</p> <p>Agency will discuss available services with the Office of Risk Management if the agency suspects or determines that a breach of information has occurred.</p> <p>References: None</p>
IR-8 Incident Response Plan	<p>Agency will develop an incident response plan that provides the agency with a roadmap for implementing its incident response capability that includes:</p> <ul style="list-style-type: none"> – Meeting the unique requirements of the agency, which relate to mission, size, structure, and functions – Defining and aligning reportable incidents based on ITA Policy, Standards, and Guidelines, and Idaho Statute – Developing metrics for measuring the incident response capability within the agency – Utilizing the VERIS taxonomy

	<ul style="list-style-type: none"> – Defining the resources and management support needed to effectively maintain and mature an incident response capability – Reviewing and approving the plan by <i>Incident Response Team Members</i> – Distributes copies of the incident response plan to the Incident Response Team Members – Reviews and updates the incident response plan at least annually <p>Note: ITS will be responsible for incident response planning for ITS customers.</p> <p>References: NIST SP 800-61</p>
IR-9 Information Spillage Response	Not required at this time, may be implemented at an agency's discretion.
IR-10 Integrated Information Security Analysis Team	Not required at this time, may be implemented at an agency's discretion

B. Vocabulary for Event Recording and Information Sharing (VERIS)

All agencies will adopt the VERIS framework for its incident response documentation and intelligence sharing. A hardcopy of the VERIS Reporting Form is available now from ITS or Office of Risk Management.

C. WebEOC

All agencies will utilize the WebEOC application as the platform to report incidents and breaches for notification purposes and incident and breach intelligence sharing.

V. REFERENCE DOCUMENTS

- Idaho Code §§ [28-51-104](#), [28-51-105](#), [28-51-106](#), and [28-51-107](#); Definitions, Disclosure of Breach of Security of Computerized Personal Information by an Agency, Individual or Commercial Entity, Procedures Deemed in Compliance with Security Breach Requirements, and Violations respectively
- ITA Policy [P4110](#) Agency IT Security Coordinator
- ITA Policy [P4590](#) (Cybersecurity Incident and Breach Response Management and Reporting)
- ITA Guideline [G585](#) (Cybersecurity Incident and Breach Response Reporting)

- ITA Guideline [G525](#) (Cybersecurity Incident and Breach Response Management)
- NIST Special Publication [800-12](#) An Introduction to Information Security
- NIST Special Publication [800-16](#) Information Technology Security Training Requirements: A Role- and Performance-Based Model
- NIST Special Publication [800-50](#) Building an Information Technology Security Awareness and Training Program
- NIST Special Publication [800-53r4](#) Incident Response Family Security and Privacy Controls for Federal Information Systems and Organizations
- NIST Special Publication [800-61r2](#) Computer Security Incident Handling Guide
- NIST Special Publication [800-83r1](#) Guide to Malware Incident Prevention and Handling for Desktops and Laptops
- NIST Special Publication [800-84](#) Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities
- NIST Special Publication [800-100](#) Information Security Handbook: A Guide for Managers
- NIST Special Publication [800-115](#) Technical Guide to Information Security Testing and Assessment
- NIST FIPS Publication [199](#) Standards for Security Categorization of Federal Information and Information Systems

VI. CONTACT INFORMATION

For more information, contact the ITA Staff at (208) 605-4064.

VII. REVIEW CYCLE

Twelve (12) months

VIII. REVISION HISTORY

06/18/2019 – Sections I and III revised; Section IV. D. deleted.

Effective Date: February 19, 2019