

Idaho Technology Authority (ITA)

ENTERPRISE GUIDELINES – G500 SECURITY PROCEDURES

Category: G525 – CYBERSECURITY INCIDENT AND BREACH RESPONSE MANAGEMENT

CONTENTS

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

I. DEFINITIONS

See ITA Guideline [G105](#) (ITA Glossary of Terms) for definitions

II. RATIONALE

This guideline assists an agency in establishing an incident response capability and maintain alignment with ITA policies, standards, and guidelines pertaining to incident and breach response management.

III. INCIDENT AND BREACH RESPONSE ROLES AND CONTACT INFORMATION

NOTE: To report an incident or breach, it is recommended an agency use ITA Guideline G585 for procedural guidance. 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">• Assists agencies 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 (ORM)	<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 (OAG)	<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. GUIDELINE

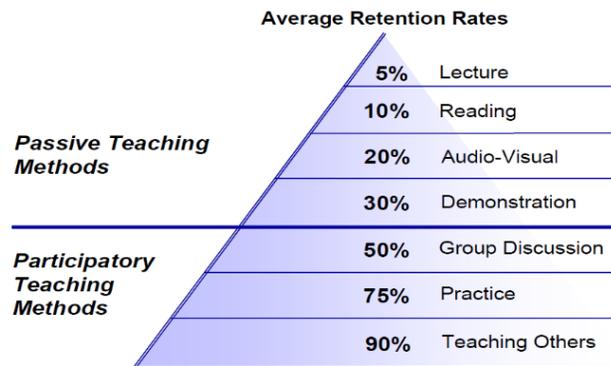
NIST SP 800-53 Family of Controls (IR-1 – IR-8)	
Control #	Guideline
Global	<p>Various team models were reviewed and discussed with ITS and agency personnel. It has been determined that the best team model to foster a coordinated and cooperative incident response handling capability is to adopt the distributed team model outlined in NIST Computer Security Incident Handling Guide SP 800-61 Revision 2.</p> <p>The distributed model supports:</p> <ol style="list-style-type: none"> 1. An enterprise that has multiple incident response teams, each responsible for a logical or physical segment of the enterprise (such as agencies). 2. A federated model that has distributed teams (agencies) that are still part of a single coordinated entity (ITS) so that the incident response capability is consistent across all agencies and information/intelligence is shared among teams. 3. An agencies autonomy and unique needs while at the same time allowing them to participate in the centralized process. <p>References: NIST SP 800-61</p>
IR-1 Incident Response Policy and Procedures	<p>Agencies should align policies and procedures with ITA policies, standards, and guidelines. Additionally, the agency should seek endorsement of their policies and procedures from their Senior leadership which promotes a tone from the top that has a positive effect on behavioral change and compliance.</p> <p>References: NIST SP 800-12, 800-61, 800-83, 800-100</p>

IR-2
Incident
Response
Training

To help ensure employees are always ready to recognize an adverse event and report an incident, and for an agencies incident response handler to respond to an incident, an agencies incident response training program should be geared towards a combination of training methods that help provide a high-level of retention.

Learned skills for end users and incident response handlers can perish quickly (typically about 3 months after training). Therefore, it is important to consider how frequent training is being delivered to keep end-users alert and incident handling skills fresh.

Below is a diagram illustrating retention rates of various training methods to assist an agency in developing an effective training strategy.



*Adapted from National Training Laboratories. Bethel, Maine

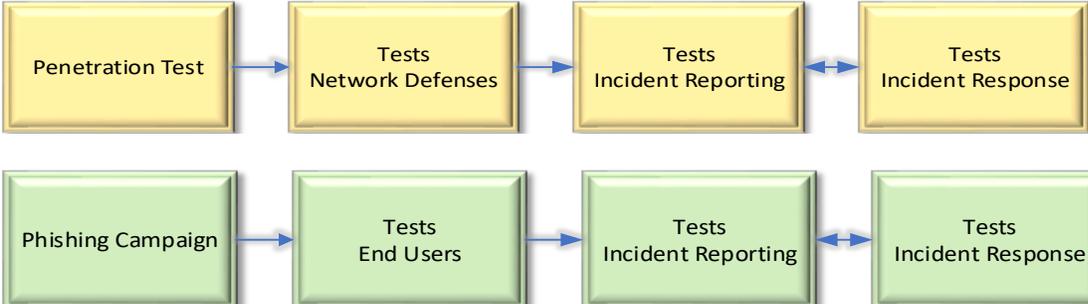
Training topic examples for Incident Response personnel are (but not limited to):

1. Policy and procedures review
2. Incident handling (documentation, forensics, etc.)
3. Procedure walk-throughs
4. Playbook reviews
5. Job-aids
6. Professional training (SANS, InfoSec, etc.)

End-user training topic examples are (but not limited to):

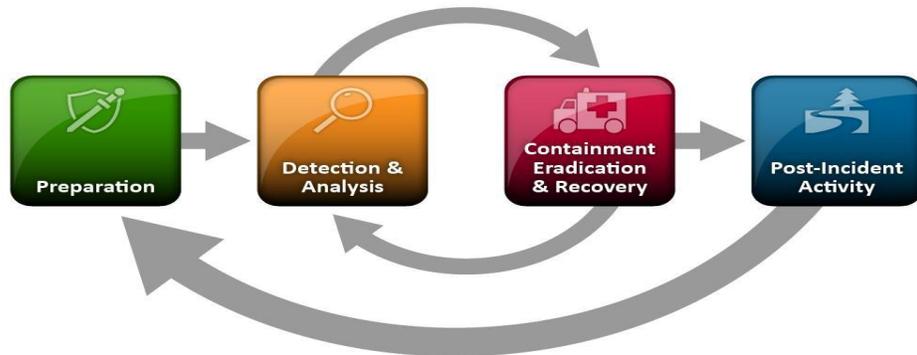
1. Policy and procedures review
2. Job-aids for reporting an incident
3. Cybersecurity posters
4. Training designated on how to recognize an adverse event
5. Informal lunch sessions
6. Online training

To prevent incidents and breaches, a training program can also consider:

	<ul style="list-style-type: none"> - Mistakes employees make such as: <ul style="list-style-type: none"> o Using weak passwords o Poor data handling o Sensitive information left on desk (clean desk policy) o Tailgating o Poor use of agency resources (i.e. social engineering, peer-to-peer file sharing, etc.) <p>Finally, in developing a good training program an agency can also consider metrics derived from their information systems such as:</p> <ul style="list-style-type: none"> - # social engineering incidents - # of unauthorized information systems or devices connected - # of malware/virus incidents - # of policy violations <p>NOTE: It is important for an agency to consider their regulatory requirements when developing their training strategy.</p> <p>References: NIST SP 800-16, 800-50</p>
<p>IR-3 Incident Response Testing</p>	<p>Testing the incident response capability can uncover weaknesses in the incident response capability and provide valuable information to improve training efforts. Testing employees and the incident response team on what to do and how to do it helps ensure perishable skills are reinforced and maintained.</p> <p>At a minimum, phishing campaigns to test employees and penetration tests to test network defenses (both scheduled and unscheduled) should be conducted <i>at least annually</i> (preferably semi-annually or quarterly) and should test the entire process from attack to response (see below).</p>  <p>Testing examples are (but not limited too):</p> <ol style="list-style-type: none"> 1. Table-top exercises for incident response handlers 2. Walk-throughs for incident response handlers 3. Phishing campaigns to test end users <p>References: NIST SP 800-84, 800-115</p>

IR-4
Incident
Response
Handling

The incident handling phases mentioned in ITA Enterprise Standard S6010 provide a phased approach in managing incidents and breaches. The following information is a breakout of the various handling phases and what should be considered in each of them.



Source: NIST SP 800-61 Rev. 2 – Computer Security Incident Handling Guide

Preparation Phase

The preparation phase includes steps taken before an incident occurs. These include:

- a. Documenting incident response policies and procedures.
- b. Providing tools for remediation and forensics
- c. Escalation procedures
- d. Incident tracking system
- e. Asset documentation (network diagrams, port lists, baselines, privilege accounts, image files, etc.)
- f. Incident handlers training plan.
- g. Communication plan for normal and after-hours.

Detection and Analysis Phase

Identify the attack vectors:

- a. External Media – Lost, stolen, etc.
- b. Attrition – DDOS, password cracking, buffer overflow, etc.
- c. Web – Cross-site scripting, etc.
- d. Email – Phishing, etc.
- e. Impersonation – Rogue access devices, man-in-the-middle, etc.
- f. Improper usage – Unauthorized software, blacklisted URLs, etc.
- g. Loss or theft of equipment
- h. Other

Containment, Eradication, and Recovery

Criteria for determining the appropriate strategy include:

- a. Potential damage to and theft of resources
- b. Need for evidence preservation
- c. Service availability

	<ul style="list-style-type: none"> d. Time and resources available to implement strategy e. Effectiveness of the strategy f. Duration of the solution <p><u>Post-Incident Activity</u></p> <p>Capture the essential elements of the incident:</p> <ul style="list-style-type: none"> a. What happened and time of occurrence b. Documented procedures adequate and followed c. Information needed sooner d. Inhibitors e. Staff adequate f. Information sharing g. Identification of controls to prevent incident reoccurring h. Precursors or indicators of attack i. Additional incident life cycle resources needed <p>Agencies have the flexibility to use other best practice-based incident handling guides that follow a similar phased process such as those from the SANS Institute which follow a similar phase approach.</p> <p>It is important that the agency establishes/considers activities such as chain of custody, order of volatility, and for continuous improvement; lessons learned activities.</p> <p>NOTE: Incident response playbooks are also available for agencies to use and tailor. These playbooks provide valuable information for phishing, malware, ransomware, etc. utilizing a best practice phased methodology.</p> <p>References: NIST SP 800-61</p>
<p>IR-5 Incident Response Monitoring</p>	<p>This control addresses how incidents are investigated, documented, and managed using various tools such as incident response playbooks, the VERIS reporting form, and the electronic incident response reporting form within those phases.</p> <p>Incidents and breaches will be documented using the VERIS reporting form, which is based on the VERIS framework. This establishes a common language for documenting incident/breach events throughout the enterprise.</p> <p>It is recommended that agencies adopt a “checklist” similar to the one found in NIST SP 800-61 as a guide to ensure that all handling phases are considered during an incident or breach and included with their investigation documentation.</p>

	<p>Monitoring incidents includes maintaining records about each incident, updating status of the incident, and other pertinent information necessary for forensics, chain of custody, evaluating incident details, trends, and handling.</p> <p>References: NIST SP 800-61</p>
<p>IR-6 Incident Response Reporting</p>	<p>Reporting contains two primary areas of focus:</p> <ol style="list-style-type: none"> 1. <u>Technical Reporting</u>: Involves documenting and reporting the technical details of an incident or breach as soon as possible – preferably starting when detected. 2. <u>Non-technical Reporting</u>: Involves alerting agency and/or enterprise stakeholders of the incident or breach. <p>Refer to ITA Enterprise Guidelines G585 for recommended steps on incident and breach reporting.</p> <p>References: NIST SP 800-84, 800-115</p>
<p>IR-7 Incident Response Assistance</p>	<p>The Office of Risk Management (ORM) and ITS can assist an agency in the event they experience an incident or breach.</p> <p>ORM can assist an agency by determining if the agency is eligible for the State of Idaho’s cyber liability insurance program.</p> <p>Cyber liability insurance covers liability for a data breach in which the agencies customers' personally identifiable information (PII), such as Social Security or credit card numbers, is exposed or stolen by a hacker or other criminal who has gained access to the agencies electronic network.</p> <p>For more information regarding cyber liability insurance, contact the Office of Risk Management. ITS can provide technical assistance and coordination during an incident.</p> <p>References: None</p>
<p>IR-8 Incident Response Plan</p>	<p>On an annual basis, a State-wide incident response planning meeting will occur. During this meeting, lessons learned from the year and other relevant information will be discussed to determine which of the eight (8) controls (and other information) in the State of Idaho’s incident response program need to be revised or improved.</p> <p>It is recommended that each agency, prior to this meeting, conduct their own annual lessons learned meeting to discuss the controls they would like to see improved or revised.</p> <p>Common topics for review are, but not limited to:</p> <ol style="list-style-type: none"> 1. Incident response controls 1-8 2. Lessons learned from incidents and breaches

	<p>3. Improvements or refinements to the reporting process, including the incident response form</p> <p>4. Improvements or refinements to VERIS, including the VERIS reporting form</p> <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	May be implemented at the agency's discretion.
IR-10 Integrated Information Security Analysis Team	May be implemented at the agency's discretion.

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 Standard [S6010](#) (Cybersecurity Incident and Breach Response Management and Reporting)
- ITA Guideline [G585](#) (Cybersecurity Incident and Breach Response Reporting)
- 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

VI. CONTACT INFORMATION

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

VII. REVIEW CYCLE

Twelve (12) months

VIII. REVISION HISTORY

Effective Date: February 19, 2019