Idaho Technology Authority (ITA)

ENTERPRISE STANDARDS – S6000 SECURITY

Category: S6010 – Cybersecurity Incident and Breach Response Management and Reporting

CONTENTS:

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.

For all other definitions of terms, see ITS Guideline G105 (Glossary of Terms).

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. APPROVED STANDARD

Idaho Code §§ 28-51-104, 28-51-105, 28-51-106, and 28-51-107 applies to any city, county or state agency, individual or a commercial entity that conducts business in Idaho and that owns or licenses computerized data that includes personal information about a resident of Idaho.

Pursuant to Idaho Code §§ 28-51-104, 28-51-105, 28-51-106, and 28-51-107, all state agencies must report incidents and breaches. This Standard requires State agencies to file a report for cyber incidents and breaches within WebEOC as a method of notification and to aide in intelligence gathering and sharing.

Note: Federal data regulations may require separate or additional actions.

Breach Reporting: Regardless of the determination of misuse, agencies have a responsibility to notify the Attorney General's Office (OAG), the Office of Risk Management (ORM), and the Office of Information Technology Services (ITS) no later than 24 hours after discovery of a breach.

Incident Reporting: Within five (5) business days of discovery, agency will report incidents to ITS CISO Office utilizing WebEOC. 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 to ITS CISO Office at the conclusion of the investigation.

All state agencies will use the State of Idaho Incident Response Reporting Handbook (appended below).

NOTE: ITS customers will notify ITS via the ITS Service Desk which will notify the CISO of the breach. The CISO will immediately log the breach into WebEOC.

IV. PROCEDURE REFERENCE

- 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)

- 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 800-53r5 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 800-84 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

V. REVIEW CYCLE

Twelve (12) Months

VI. CONTACT INFORMATION

For more information and to request documentation from the State CISO pertaining to this standard, contact the ITA Staff at (208) 605-4064

VII. ADDITIONAL INFORMATION - EXEMPTION PROCESS

Refer to ITA Policy P1010 (IT Policies, Standards, and Guidelines Framework).

REVISION HISTORY

07/23/2025 - Revised for ADA compliance

04/20/2021 - Clarified Section III for consistency with Idaho Statute; added WebEOC for reporting requirements; Section IV updated for reference; added attachment.

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

Effective Date: February 19, 2019

ATTACHMENT

State of Idaho Incident Response Reporting Handbook

State of Idaho

Incident Response Reporting Handbook

The process outlined in this handbook is in addition to any regulatory reporting requirements.

Revision 1.03
10/16/2020

IDAHO

Table of Contents

This Handbook supersedes:

G525 – CYBERSECURITY INCIDENT AND BREACH RESPONSE MANAGEMENT

G585 – CYBERSECURITY INCIDENT AND BREACH RESPONSE REPORTING

I. GLOSSARY OF TERMS

See ITA Guideline G105 (ITA Glossary of Terms) for definitions

II. RATIONALE

This handbook is designed to assist agencies to establish incident response reporting procedures in alignment with Idaho State statute and policies pertaining to incident and breach response reporting. All agencies will utilize the WebEOC service provided as the platform to report events, incidents and breaches for notification purposes. This also aides in incident and breach intelligence sharing and is required to obtain cyber insurance.

III. ROLES AND CONTACT INFORMATION

Service Desk		ITS – CIO	(208)605-4185
Security Operations		ORM	(208)332-1869
IRT		Required Agencies	
CISO			
CIO			
Executive Staff			
Legal – AG			
PIO			

Agency Contact Numbers
Fill in this table with your agency contact information for quick reference.

IV. DEFINITIONS AND QUICK REFERENCE

Incidents are always events, but events are not always incidents.

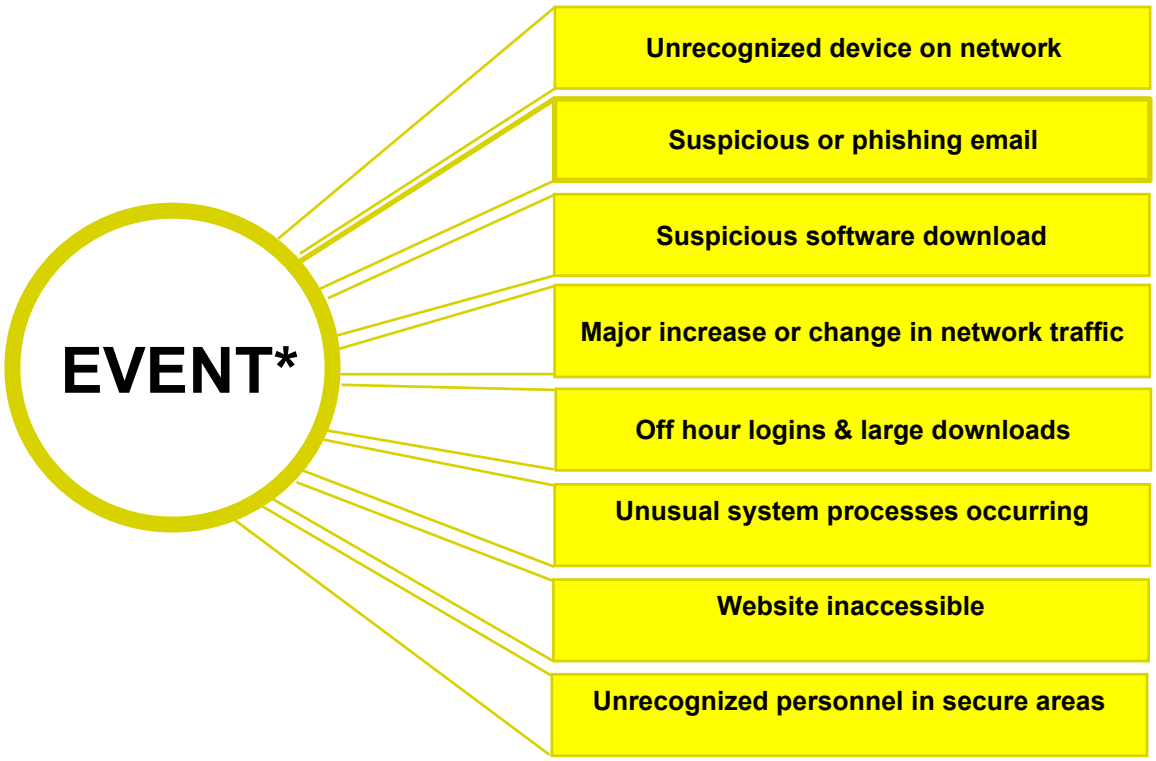
Cybersecurity Event

A Cybersecurity event is defined as any observable anomaly in a network, information system or state agency facility.

1. Agencies may escalate an event to the CISO Office in ITS for assistance and/or for community awareness.

2. The CISO Office in ITS will distribute awareness communications to other state entities and partners such as DHS and/or MS-ISAC for their threat intelligence needs.

3. Agencies are encouraged to report significant cybersecurity events, such as a phishing campaign. ITS CISO Office will review and determine if an event should be escalated.



* These are examples of a Security Event – this is not a complete list.

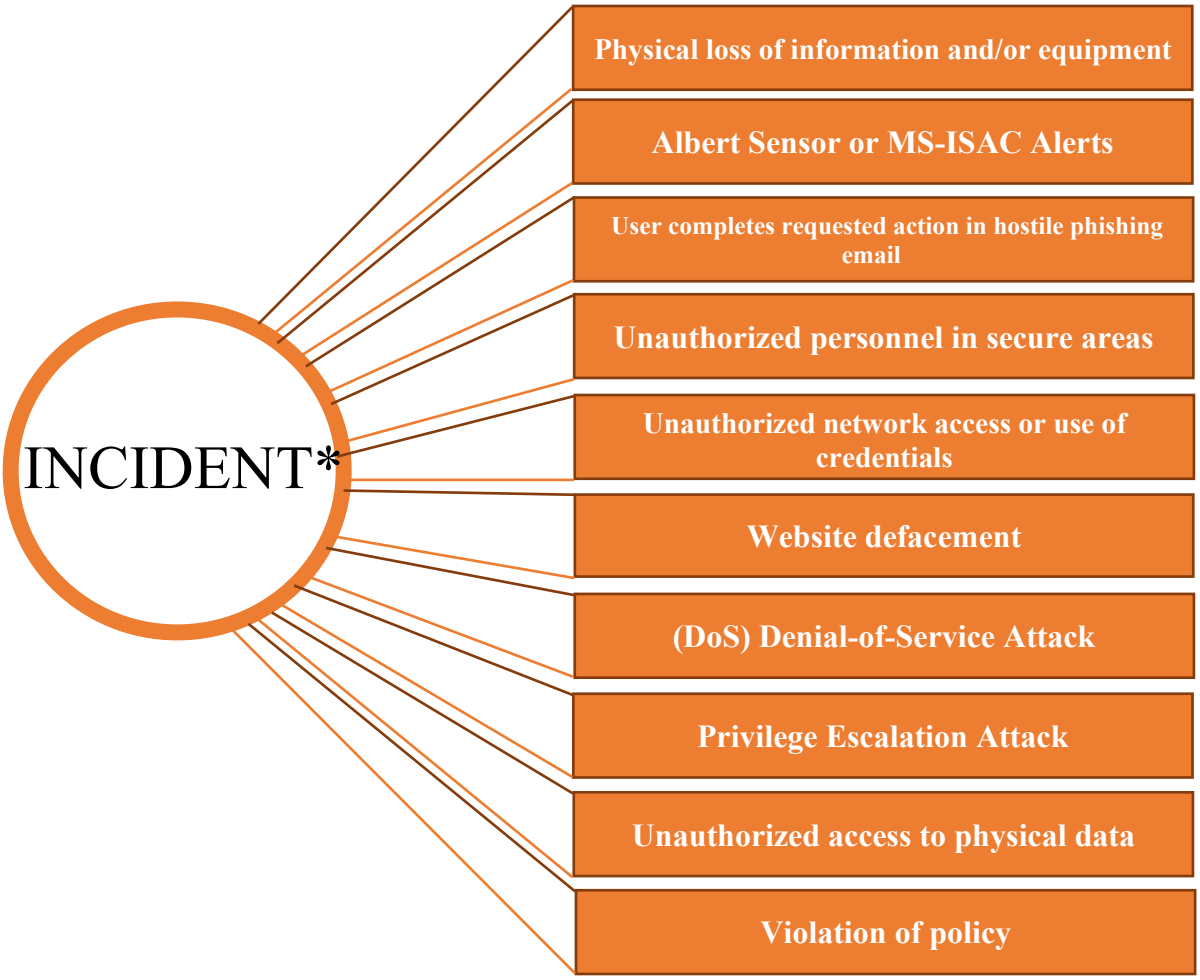
Cybersecurity Incident

A cybersecurity Incident is defined as an event that impacts the confidentiality, integrity or availability of data, a network, or system or breach of policy.

All cybersecurity incidents must be reported using WebEOC.

Reports are required:

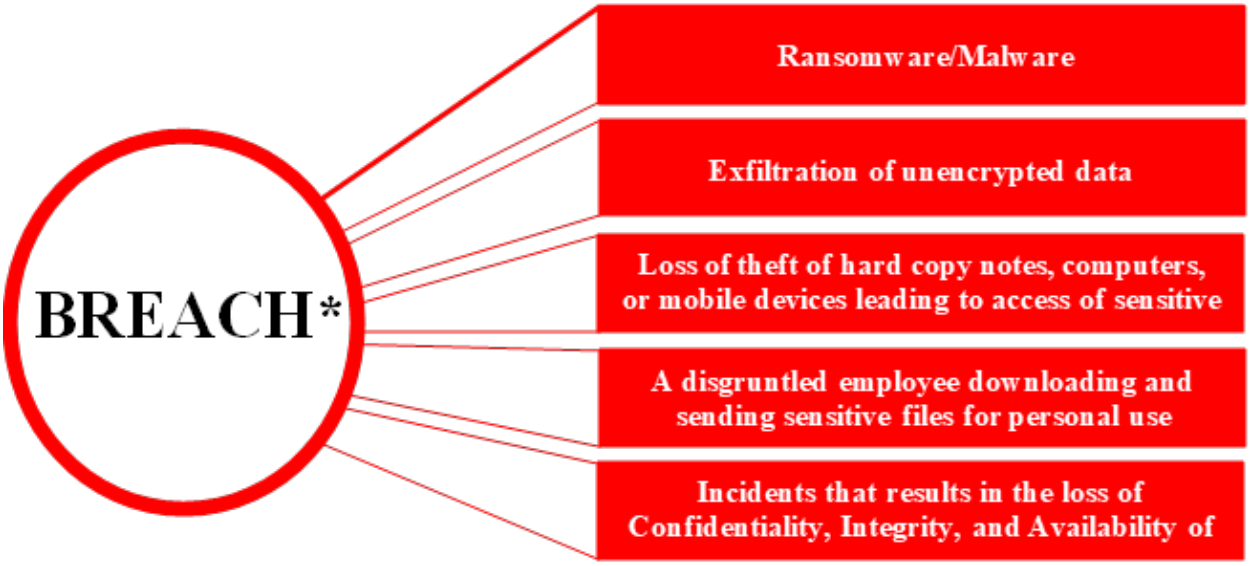
1. At the discretion of the State or Agency CISO Office.
2. In case of a data loss. Any exposure of proprietary or sensitive unencrypted information through either data theft or data leakage.
3. For any verified Albert Sensor alerts that are relayed to an agency from ITS.



*These are examples of a Security Incident – this is not a complete list.

Cybersecurity Breach

All cybersecurity breaches must be reported using WebEOC. Per Idaho Statute §§ 28-51-104, a data breach means "the illegal acquisition of unencrypted computerized data that materially compromises the security, confidentiality, or integrity of personal information for one (1) or more persons maintained by an agency, individual or a commercial entity."



*These are examples of a Security Breach – this is not a complete list

V. NAVIGATING WEBEOC

Incidents will be investigated by the owning agency and must be reported to the ITS CISO Office via **WebEOC** or at https://ioem.idaho.gov/webeoc/.

***WebEOC reports must be completed to record the incident with ITS and to meet timing requirements for cyber insurance, should the event develop into an incident or evolve into a breach.**

WebEOC log in instructions can be found here.

***DO NOT input affected user information when completing the form.**

1. Initial WebEOC reports must include the following about the incident:
    a. Under the [Incident Tracking] tab
        (1) Incident Type
        (2) Incident Summary
    b. Under the [Discovery and Response] tab
        (1) When did the incident occur?
    c. Under the [Actions] tab
        (1) What kind of incident is it? (Choose your best guess, this can change).
    d. All other information you have on the incident.
2. Agencies will monitor the incident and provide periodic updates.
3. Agencies will report the timely closure of an incident in WebEOC.

WebEOC application and account creation support – Karl DeHart 208-869-1404 or email kdehart@bhs.idaho.gov.

VI. 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.

VII. TIMING REQUIREMENTS

1. Events

    Agencies can escalate an event to the CISO Office in ITS for assistance and/or for community awareness.

2. Incidents

Within five business days of discovery, agency will report incidents to ITS CISO Office utilizing WebEOC. 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 to ITS CISO Office at the conclusion of the investigation.

If a full investigation requires more than 30-days, contact ITS.

3. Breaches

   A. Regardless of the determination of misuse, agencies have a responsibility to notify the Attorney General's Office (OAG), the Office of Risk Management (ORM), and the Office of Information Technology Services (OITS) no later than 24 hours after discovery of a breach.

NOTE: ITS customers will notify ITS via the ITS Service Desk which will notify the CISO of the breach. The CISO will immediately log the breach into WebEOC.

   B. Per Idaho Code §§ 28-51-105, an agency has a responsibility to notify all parties that are affected by the breach or could potentially be affected by the breach.

There are different requirements associated with each of these notifications, both of which are addressed below. Notification to OAG, ORM and ITS are made by:

1. Contacting the Deputy Attorney General that advises the agency or calling the Attorney General's Office if the agency does not have an assigned Deputy Attorney General.
2. Completing the incident response form (WebEOC) with investigation information that describes the breach, AND by alerting the ORM and ITS of the breach by calling:
   a. ORM at 208-332-1869, and
   b. ITS at 208-605-4000

Agency responsibilities for notifying affected parties:

1. Notification to affected parties shall be made expediently and without unreasonable delay following the discovery of a cybersecurity breach if the agency believes that the information has or will be misused. Notification to affected parties must be consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach, to identify the individuals affected, and to restore the reasonable integrity of the computerized data system.
2. Notifications may be delayed when a law enforcement agency determines that notification would impede a criminal investigation. In such a case, notice must

be made as soon as possible after a law enforcement agency advises the notification will no longer impede the investigation.

3. At the discretion of the agency, the agency can also utilize the counsel provided from ORM and/or the OAG in determining whether notification to affected Idaho residents should be delayed for purposes of investigation.
4. Refer to the "Notice" definition in §§ 28-51-104 for notice requirements.

In considering notification responsibilities, the agency must also consider:

1. The policies, rules, and regulations established by the agency's primary or functional federal regulator.

VIII. REFERENCE DOCUMENTS

- To access WebEOC go to: https://ioem.idaho.gov/webeoc/.
- 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)

IX. REVIEW CYCLE

Twelve (12) months

X. APPENDICES

1. Cybersecurity Breach Notification Sample Letter
2. Incident Handling Checklist Example
3. Incident Log Example

1. Cybersecurity Breach Notification Sample Letter

Dear _____,

We are writing because of a recent security incident at *[name of organization].*

[Describe what happened in general terms, what type of personal information was involved, and what you are doing in response.]

To protect yourself from the possibility of identifying theft, we recommend that you immediately contact *[credit care or financial account issuer]* at *[phone number]* and close your account. Tell them that your account may have been compromised. If you want to open a new account, ask *[name of account issuer]* to give you a PIN or password. This will help control access to the account.

To further protect yourself, we recommend that you place a fraud alert on your credit files. A fraud alert lets creditors know to contact you before opening new accounts. Just call any one of the three credit reporting agencies at a number below. This will let you automatically place fraud alerts with all of the credit reporting agencies. You will then receive letters from all of them, with instructions on how to get a free copy of your credit report from each.

Experian	Equifax	TransUnion
888-397-3742	888-548-7878	800-916-8800

For more information on identify theft, we suggest that you visit the Federal Trade Commission at www.consumer.gov/idtheft. If there is anything *[name of organization]* can do to assist you, please call *[toll-free number].*

[Closing]

2. Incident Handling Checklist Example

Incident Handling Checklist	
PHASE 1: IDENTIFICATION: Identification involves determining whether an incident has occurred, and if one has occurred, determining the nature of the incident. These steps should be taken in the identification phase:	
Determine whether an event is an incident. Check for simple mistakes such as errors in system configuration or an application program, hardware failures, and most commonly, user or system administrator errors.	
Identify and assess the initial evidence in detail.	
Notify appropriate officials such as supervisors or managers.	
Assign a person to coordinate the incident handling efforts.	
Coordinate with the System Owner and Service Desk to ensure needed technical support during investigation.	
Start an incident handling log. Document all actions to include date, time, and employee who performed actions. This may be needed for reporting purposes or if legal\personnel actions need to be taken.	
PHASE 2: CONTAINMENT: During this phase, the goal is to limit the scope and magnitude of an incident in order to keep the incident from getting worse. These steps should be taken in the containment phase:	
Go to physical location of system if possible. Try to limit remote access into the machine to avoid potentially compromised code. Intruders may install Trojan horses and similar malicious code in system binaries.	
Determine the risk of continuing operations. Remove system from network if deemed too risky to continue operation. If trying to preserve evidence of malware on the system, do not power down.	
If destructive processes are running, photograph the screen, then remove the power cord (from a workstation or server) or battery (from a laptop or other mobile device). Document the exact date and time, reason that the action was taken and include the photograph or reference to its location in the documentation.	
IF incident has affected any systems that contain FTI or PII – Chief Security Officer will coordinate notification and reporting.	
Determine if there is a need to have a forensics investigator brought in.	
PHASE 3: ERADICATION: This phase ensures that the problem is eliminated and vulnerabilities that allow re-entry to the system are eliminated. These steps should be taken in the eradication phase:	
Use Agency approved malware removal tools.	
If tools will not eradicate the malware then system will need to be reimaged. **Do Not reimage if evidence needs to be preserved.**	
PHASE 4: RECOVERY: This phase ensures that the system is returned to a fully operational status. These steps should be taken in the recovery phase:	
Restore the system.	
Validate the system. Once the system has been restored, verify that the operation was successful, and the system is back to its normal condition.	
Decide when to restore operations. Management may decide to leave the system offline while operating system upgrades and patches are installed.	

Monitor the systems. Once the system is back online, continue to monitor for back doors that escaped detection.	
PHASE 5: FOLLOW-UP: This phase is important in identifying lessons learned that will prevent future incidents.	
Develop a detailed incident report and provide copies to management.	
Send recommended changes to management.	
Implement approved actions.	

1. Incident Log Example

Use this as a guide to gather the information needed to input into WebEOC

Reported by: Name: Phone: E-mail:
Date & Time of incident detection:
Nature of Incident: ☐ Denial of Service ☐ Unauthorized Access ☐ Malicious Code (worm, virus) ☐ Website Defacement ☐ Scans and Probes ☐ Other (describe)
Incident description (What were the signs?):
Details: (e.g. virus name, events, etc)
Business Impact (e.g. what information or services are impacted?)
Course of action:
Additional notes: