Idaho Technology Authority (ITA)

ENTERPRISE POLICY – P4500 COMPUTER AND OPERATIONS MANAGEMENT

Category: P4580 – CYBERSECURITY INCIDENT MANAGEMENT

CONTENTS:

I. AUTHORITY

Authority: Idaho Code § 67-5745 (C)(3)

II. ABSTRACT

Information security incidents are commonplace in today's technology rich environments making an effective incident management plan a critical component of an agency's information technology program. Effective incident response is complex and requires detailed planning coupled with a significant allocation of resources. This policy assists State of Idaho agencies in establishing internal incident management plans and identifying agency collaborative responsibilities with the Statewide Cyber Security Coordinator and the Statewide Cyber Security Incident Response Team.

III. DEFINITIONS

Information Security Incident – A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

Incident Handling – The mitigation of violations of security policies and recommended practices.

Precursor: A sign that an attacker may be preparing to cause an incident.

Profiling: Measuring the characteristics of expected activity so that changes to it can be more easily identified.

Signature: A recognizable, distinguishing pattern associated with an attack, such as a binary string in a virus or a particular set of keystrokes used to gain unauthorized access to a system.

Social Engineering: An attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks.

Threat: The potential source of an adverse event.

Vulnerability: A weakness in a system, application, or network that is subject to exploitation or misuse.

IV. POLICY

This policy ensures that state agencies design and implement a cybersecurity incident response management plan that is actionable and verifiable. An incident management plan provides agency roles and responsibilities and prescribes procedures to effectively prepare, detect, contain and analyze, repair, and conduct post-incident analysis. A key component that must also be addressed by a cybersecurity incident management plan addresses reporting requirements mandated through applicable State and Federal laws, Executive Orders. Directives, policies, regulations, standards and guidance.

This policy is structured to provide an overview of incident management plan capabilities, the key phases of incident life-cycle management, an incident management process model, and reporting requirements.

Incident Management Plan Capabilities

Agency incident management plans shall provision the capabilities to include the following actions:

a. Creating an incident response policy
b. Developing procedures for performing incident handling and reporting
c. Setting guidelines for communicating with outside parties regarding incidents
d. Selecting a team structure and staffing model
e. Establishing relationships and lines of communication between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies)
f. Determining what services the incident response team should provide
g. Staffing and training the incident response team.
h. Develop an internal and external communications plan (see Figure 1. Security Incident Communications Plan).

Figure 1. Security Incident Communications Plan

Incident Management Process

The incident management process consists of preparation, detection & analysis, Containment, Eradication & Recovery, and Post-Incident Activity (see Figure 2. Incident Response Life Cycle). Agencies are required to develop internal policies and procedures for inclusion in their incident response management plan that support the Incident Response Life Cycle.

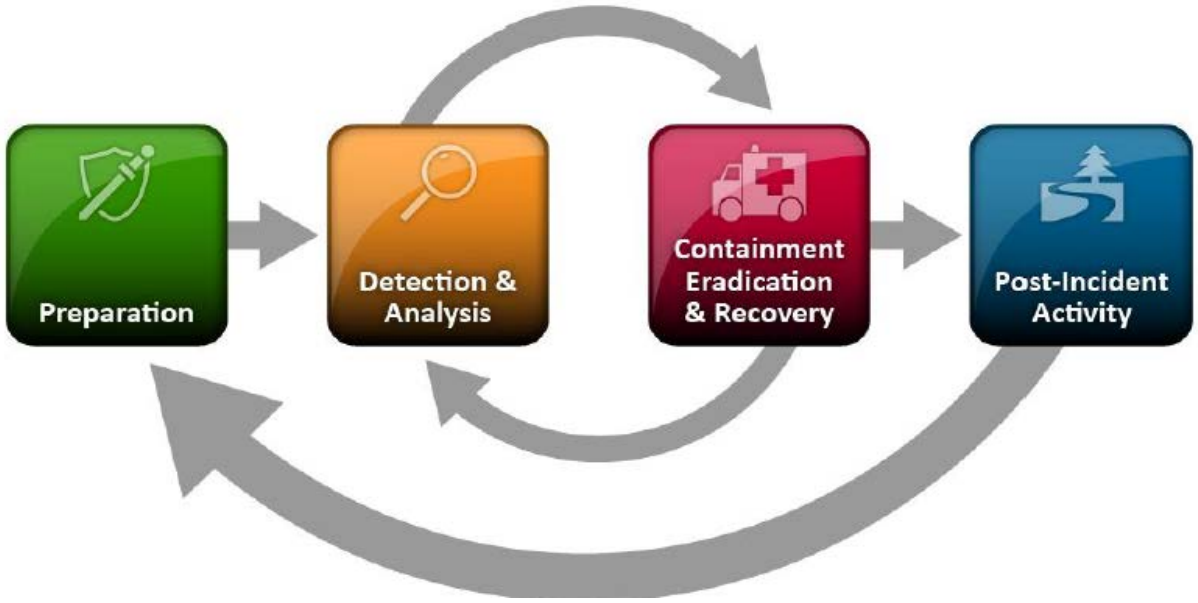

Figure 2. Incident Response Life Cycle

1) Preparation – agencies establish an incident response capability by identifying:
   a) Communication plan for normal and after-hours.
   b) Escalation Procedures

c) Incident Tracking System
d) Asset Documentation (network diagrams, port lists, baselines, privilege accounts, image files, etc.)
e) Incident handlers training plan.

2) Detection and Analysis – identify the attack vectors:
   a) External Media – lost or 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 shareware, blacklisted URLs, etc.
   g) Loss or Theft of Equipment
   h) Other

3) Containment – Criteria for determining the appropriate strategy include;
   a) Potential damage to and theft of resources
   b) Need for evidence Preservation
   c) Service Availability
   d) Time and resources available to implement strategy
   e) Effectiveness of the strategy
   f) Duration of the solution

4) Post-Incident – Capture the essential elements of the incident
   a) What happened and time of occurrence
   b) Documented procedures adequate and followed
   c) Information was needed sooner?
   d) Inhibitors
   e) Staff adequate
   f) Information Sharing Correct
   g) Identification of controls to prevent incident reoccurring
   h) Precursors or indicators of attack
   i) Additional incident life cycle resources needed

Incident Management Reporting

Agencies will include incident reporting procedures within the incident management plan in accordance with ITA Policy P4510 (Cybersecurity Incident Reporting), which was developed to facilitate external agency reporting to the approved state reporting authority. Reporting incidents provides valuable situational awareness to external organizations and the feedback for the incident reporting as part of their analysis and in identifying lessons learned.

V. EXEMPTION PROCESS

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

VI. PROCEDURE REFERENCE

NIST Special Publication 800-61 (Rev. 2) (Computer Security Incident Handling Guide)
ITA Policy P4510 (Cybersecurity Incident Reporting)
ITA Guideline G510 (Cybersecurity Incident Reporting Classification)
ITA Guideline G520 (Cybersecurity Incident Handling)
ITA Guideline G580 (Cyber Security Breach Notification)

VII. CONTACT INFORMATION

For more information, contact the ITA Staff at (208) 332-1876.
To report an incident, send email to: security@cio.idaho.gov or call (208) 332-1510.

REVISION HISTORY

Effective Date: February 23, 2016