# Idaho Technology Authority (ITA)

# ENTERPRISE POLICY – P4500 COMPUTER AND OPERATIONS MANAGEMENT

**Category: P4510 – CYBER SECURITY INCIDENT REPORTING**

**CONTENTS:**



## I. AUTHORITY

Authority: Idaho Code § 67-5745(C)(3)

## II. ABSTRACT

Establish the process for State agencies to report cyber security incidents to the Statewide Cyber Security Coordinator and the Statewide Cyber Security Incident Response Team. Reporting incidents to a central location promotes collaboration and information sharing with other entities that may be experiencing the same problems. Benefits of this policy include:

1. Improved coordination among agencies experiencing similar incidents to more accurately assess, identify, protect, and resolve problems;

2. Early warning and sharing of preventative information to help other agencies protect themselves from similar attacks;

3. Collection of information from across agencies on the types of vulnerabilities that are being exploited, frequency of attacks, and costs associated with recovering from an attack; and

4. Coordination among entities to work with law enforcement and pursue legal actions against the intruder;

5. Gain a more accurate picture of the threat facing state agencies by having a broader set of information available to incident responders (e.g. response may be different if a low level malware event simultaneously shows up on multiple agency systems).

## III. DEFINITIONS

Cyber Security Incident – Any adverse event that threatens the confidentiality, integrity or availability of an agency's information resources. These events include, but are not limited to, the following:

1. Attempts (either failed or successful) to gain unauthorized access to a system or its data;

2. Disruption or denial of service;

3. Unauthorized use of a system for the transmission, processing or storage of data;

4. Changes to system hardware, firmware or software without the agency's knowledge, instruction or consent;

5. Attempts to cause failures in critical infrastructure services or loss of critical supervisory control and data acquisition (SCADA) systems;

6. Attempts to cause failures that may cause loss of life or significant impact on the health or economic security of the agency and/or State; and

7. Probing of any nature that an agency or other authorized entity has not approved in advance for system security testing purposes.

## IV. POLICY

1. The appointed Agency IT Security Coordinator, or alternate (refer to ITA *Policy 4110 – Agency IT Security Coordinator*), will submit timely cyber security incident reports to the Statewide Cyber Security Incident Response Team in accordance with ITA *Guideline 510 – Cyber Security Incident Reporting Classification Template*. Conversely, the Statewide Cyber Security Incident Response Team will notify the applicable Agency IT Security Coordinator (or alternate) of any suspected incidents that may impact that agency's network and/or systems.
    a. Urgent Incidents - Report urgent incidents to the Statewide Cyber Security Incident Response Team (24 hours a day/7 days per week) indicating a cyber-security emergency. Reports of these incidents should be made as close to the time of discovery as possible.
    b. Non-Urgent Incidents - Report non-urgent incidents no later than the first business day following detection.

## V. EXEMPTION PROCESS

Refer to *Policy 1010 – Information Technology Policies, Standards, and Guidelines Framework*.

## VI. PROCEDURE REFERENCE

Cyber security incident reports should be based upon ITA Guidelines *G510 – Cyber Security Incident Reporting Classification Template*, *G520 – Cyber Security Alert Indicator, and G580 – Cyber Security Breach Notification*. Reports should include all available information listed in these procedures.

## VII. CONTACT INFORMATION

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

## REVISION HISTORY

07/31/13 – Added sub-section 5 in section II, and removed sub-sections 2-3 in section IV. Also added incident reporting contact information. pls

07/01/13 – Changed "ITRMC" to "ITA".

6/16/09 – Added Exemption Process and Revision History to this policy, changed the layout and deleted References and Timeline.

4/25/2005 – Updated to require exercising procedures every six (6) months to facilitate HIPAA compliance.

Effective Date: December 9, 2004