Idaho Technology Authority (ITA)

ENTERPRISE POLICY – P4500 COMPUTER AND OPERATIONS MANAGEMENT

Category: P4510 – CYBERSECURITY INCIDENT REPORTING

CONTENTS:

I. AUTHORITY

Authority: Idaho Code § 67-833

II. ABSTRACT

Establish the process for State agencies to report cyber security incidents to the Statewide Cybersecurity Coordinator and the Statewide Cybersecurity 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

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

IV. POLICY

1. The appointed Agency IT Security Coordinator, or alternate (refer to ITA Policy P4110 (Agency IT Security Coordinator), will submit timely cyber security incident reports to the Statewide Cybersecurity Incident Response Team in accordance with ITA Guideline G510 (Cybersecurity Incident Reporting Classification Template). Conversely, the Statewide Cybersecurity 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 Cybersecurity 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 ITA Policy P1010 (Information Technology Policies, Standards, and Guidelines Framework)

VI. PROCEDURE REFERENCE

Cybersecurity incident reports should be based upon ITA Guidelines G510 (Cybersecurity Incident Reporting Classification Template), G520 (Cybersecurity Incident Handling), and G580 (Cybersecurity 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: security@its.idaho.gov or call (208) 332-1510.

REVISION HISTORY

08/29/18 – Updated Section III. Definitions.

07/01/18 – Updated Idaho statute references.

04/24/14 – 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”.

06/16/09 – Added Exemption Process and Revision History to this policy, changed the layout and deleted References and Timeline.

04/25/05 – Updated to require exercising procedures every six (6) months to facilitate HIPAA compliance.

Effective Date: December 9, 2004