Idaho Technology Authority (ITA)

ENTERPRISE GUIDELINES – G500 SECURITY PROCEDURES

Category: G510 – CYBERSECURITY INCIDENT REPORTING CLASSIFICATION TEMPLATE

I. DEFINITION

Cybersecurity Incident: Any adverse event that threatens the confidentiality, integrity or accessibility of an agency's information resources.

II. RATIONALE

These guidelines provide a suggested classification template for agencies to use when reporting cyber security incidents, in accordance with ITA Policy P4510 – Cyber Security Incident Reporting.

III. GUIDELINE

Agencies should report cyber security incidents to the Statewide Cyber Security Incident Response Team in accordance with ITA Policy P4510 Cyber Security Incident Reporting (currently led by the Office of IT Services (ITS)).

Cyber security incidents may include, but are not limited to, the following events (regardless of platform or computing environment):

- Unauthorized access to a network, system, and/or data
- Repeated attempts at unauthorized access (from either internal or external sources)
- System changes not authorized by or known to the system owner
- Denial of Service (DoS) attack or other disruptions to service
- Evidence of tampering with, removal of, or loss of data
- Web site defacement
- Social engineering incidents

- Theft of, or non-accidental physical damage to, information systems
- Malware attacks adversely affecting servers or workstations
- Evidence of inappropriate use or other noncompliance with policies or standards
- Other incidents that could compromise the integrity of the state's information systems

State of Idaho users can report an actual or suspected cybersecurity incident by phone (208)-332-1510 or by utilizing the Cyber Incident Reporting Form located at: https://requests.intranet.idaho.gov/ReportCyberIncident.aspx

Identifying one or more of the following threat vectors will help in accurately classifying and providing the right level of response to a cyber security incident:

- Unknown
- Web
- External/Removable Media
- Improper Usage
- Other
- Attrition
- Email
- Impersonation/Spoofing
- Loss or Theft of Equipment
- Physical Cause

IV. PROCEDURE REFERENCE

Policies for *Cyber Security Incident Reporting Template* are detailed in ITA Information Technology *Enterprise Policies – P4110 – IT Security Coordinator* and *P4510 – Cyber Security Incident Reporting*.

V. 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

07/01/18 – Changed "OCIO" and "Department of Administration" to "ITS".

12/15/15 - Provides classification guidance for agency's reporting requirements replacing the outdated "rainbow" attack vector indicators.

07/31/13 – Removed event definitions from Section I. Removed subsection 3 in Section IV and removed Appendix A Reporting Template. pls

07/01/13 – Changed “ITRMC” to “ITA”.

6/16/09 – Added Procedure Reference, Contact Information and Revision History to this guideline; changed the layout and deleted References and Timeline.

Effective Date: December 9, 2004