

Information Technology Resource Management Council (ITRMC)

ENTERPRISE POLICY – P4500 COMPUTER AND OPERATIONS MANAGEMENT

Category: P4510 – CYBER SECURITY INCIDENT REPORTING

CONTENTS:

- I. [Authority](#)
- II. [Abstract](#)
- III. [Definition](#)
- IV. [Reference](#)
- V. [Policy](#)
- VI. [Procedure Reference](#)
- VII. [Contact Information](#)
- VIII. [Time Line](#)
- IX. [Revision History](#)

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 help identify, protect, and quickly 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.

III. DEFINITION

Cyber Security Incident – A cyber security incident is considered to be any adverse event that threatens the confidentiality, integrity or accessibility 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. REFERENCE

ITRMC *Guideline 510 – Cyber Security Incident Reporting Template* can be found at: <http://www2.state.id.us/itrmc/plan&policies/guidelines.htm#510>.

V. POLICY

1. The appointed Agency IT Security Coordinator, or alternate (refer to ITRMC [Policy 4110 – Agency IT Security Coordinator](#)), will submit timely cyber security incident reports to the Statewide Cyber Security Incident Response Team in accordance with ITRMC [Guideline 510 – Cyber Security Incident Reporting 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.
2. The following types of incidents will be reported:
 - A. Unauthorized access
 - (1) Report successful, unauthorized access to agency systems (e.g., web site defacements, unauthorized root/administrator access, etc.).

- (2) Report unsuccessful attempts only if they are considered to be persistent (e.g., an intruder from the same source keeps locking out accounts due to brute force password attacks, an automated script keeps probing a web server causing response problems, etc.).
- (3) Report suspected unauthorized access, even if unproven, if the agency believes that incident may impact other agencies.

B. Malicious Code

- (1) Report instances of viruses, Trojan horses, worms or other malicious code that has had wide-spread impact or adversely affected one (or more) agency mission critical server(s).
- (2) Report malicious code blocked by e-mail proxies and/or anti-virus software only if it seems to be persistent and beyond current Internet worm traffic.

C. Denial of Service (DoS)

- (1) Report all DoS attacks that adversely affect or degrade access to critical servers.
- (2) Report all other attempted DoS attacks particularly if they are persistent or significant (e.g., attempted DoS attacks aimed specifically at an agency's routers or critical servers would be considered significant).

D. Reconnaissance Scans and Probes

- (1) Scans and probes that precede or are related to the incidents listed above should be reported as part of the incident.
- (2) Any other scans and probes should be reported only if they are persistent or significant (e.g., stealth scans that attempt to avoid detection may be considered significant).

3. The Statewide Cyber Security Incident Response Team will notify the Statewide Cyber Security Coordinator of any reported incidents. The Statewide Cyber Security Coordinator may coordinate with the Multi-State Information Sharing and Analysis Center to identify any similar incidents occurring throughout the nation's other state governments.

VI. PROCEDURE REFERENCE

Cyber security incident reports should be based upon ITRMC [Guideline 510 – Cyber Security Incident Reporting Procedures](#). Reports should include all available information listed in these procedures.

VII. CONTACT INFORMATION

For more information, contact the ITRMC Staff at (208) 332-1876.

VIII. TIME LINE

Last Reviewed: April 25, 2005
Last Revised: April 25, 2005
Effective Date: December 9, 2004

IX. REVISION HISTORY

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