

# Information Technology Resource Management Council (ITRMC)

## **ENTERPRISE GUIDELINES – G500 SECURITY PROCEDURES**

**Category: G510 – CYBER SECURITY INCIDENT REPORTING TEMPLATE**

### **CONTENTS:**

- I. [Definition](#)
- II. [Rationale](#)
- III. [Reference](#)
- IV. [Guideline](#)
- V. [Timeline](#)
- VI. [Appendices](#)
  - [Appendix A](#): Cyber Security Incident Reporting Template

### **I. DEFINITION**

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

### **II. RATIONALE**

These guidelines provide a suggested template for agencies to use when reporting cyber security incidents, in accordance with *ITRMC [Policy 4510 – Cyber Security Incident Reporting](#)*.

### III. REFERENCE

1. ITRMC [Policy 4110 – IT Security Coordinator](#); and
2. ITRMC [Policy 4510 – Cyber Security Incident Reporting](#).

### IV. GUIDELINE

Agencies should report cyber security incidents to the Statewide Cyber Security Incident Response Team (currently led by the Department of Administration) in accordance with the following procedures:

1. Urgent Incidents – Report urgent incidents to the Statewide Cyber Security Incident Response Team by calling (208) 332-1850 (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. Examples of urgent incidents include:
  - A. Unauthorized root or administrator access to critical servers, routers, or firewalls (affected system should be immediately disconnected from the network until cleaned);
  - B. Wide spread virus or worm infection (affected system should be immediately disconnected from the network until cleaned);
  - C. Major outages due to denial of service attacks;
  - D. Mission critical application failures; or
  - E. Attacks on mission critical infrastructure services.
2. Non-Urgent Incidents – Report non-urgent incidents to the above contact phone number no later than the first business day following detection. Examples of non-urgent incidents include:
  - A. Major reconnaissance scans and probes;
  - B. Attempted but unsuccessful denial of service attacks; or
  - C. Degradation of service attacks.
3. Incident reports should contain as much of the following information as is available at the time of reporting. Additional information (such as staff resources expended or costs associated with the incident) may not be known initially; however, the reporting agency should track this information and report all requested information (as stated below) in a follow up report. A *Cyber Security Incident Reporting Template* (see [Appendix A](#)) is provided to assist agencies in this reporting process.
  - A. Contact Information:

- (1) Individual's name;
- (2) Agency name;
- (3) E-mail address; and
- (4) Phone number.

B. Description of Incident:

- (1) Date and time incident was detected;
- (2) Date and time incident actually occurred (if different from above);
- (3) Type of incident (e.g., web defacement, virus/worm, etc.);
- (4) Method of intrusion (e.g., vulnerability exploited), if known;
- (5) Level of unauthorized access attained (e.g., root, administrator, user, etc.), if known;
- (6) Log extracts (if appropriate and available); and
- (7) Any other relevant information.

C. Affected System(s):

- (1) IP address and hostname;
- (2) Purpose of the system (e.g., DNS server, router, e-mail server, application server, etc.);
- (3) Operating system (to include version and patch levels);
- (4) What type of applicable protection is in place (e.g., agency firewall, intrusion detection system, anti-virus, etc.);
- (5) Ports of communication, if known (e.g., TCP port 21, etc.);
- (6) Physical location of the system; and
- (7) Description of attempted attack vector(s) (e.g., services attacked or compromised).

D. Attack Source(s):

- (1) IP address and hostname;
- (2) Any other relevant information; and

- (3) Ports (or approximate range of ports) of communication used, if known (e.g., TCP port 21, UDP ports 1024-1050, etc.).

E. Damage Assessment (estimated):

- (1) Impact of attack on agency operations and/or services;
- (2) Staff time to detect, handle, and recover from the incident;
- (3) Costs due to information loss, downtime, or other costs; and
- (4) Current status of system(s) and/or network(s).

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

## **V. TIME LINE**

Last Revised:

Effective Date: December 9, 2004

**CYBER SECURITY INCIDENT REPORTING TEMPLATE**  
APPENDIX A

Contact Information	
Individual's Name	
Agency Name	
E-Mail Address	
Phone Number	

**Statewide Cyber Security  
Incident Reporting Hotline:**

**208-332-1850**

*(Available 24x7. If no answer, leave message & responder will return your phone call promptly)*

Description of Incident	
Date / Time Incident Detected	
Date / Time Incident Occurred	
Type of Incident (Examples: Web defacement, virus, etc)	
Method of Intrusion (Example: Vulnerability exploited, compromised account, etc)	
Level of Unauthorized Access Attained (Example: root, administrator, user, etc)	
Any Other Relevant Information (Attach log extracts as separate document/file)	

Affected System(s)	
<b>IP Address(es)</b>	
<b>Hostname(s)</b>	
<b>Purpose of System</b> (Example: DNS server, router, e-mail server, application server, etc)	
<b>Operating System</b> (Include version and patch levels)	
<b>Description of Protection In Place</b> (Example: Agency firewall, intrusion detection system, anti-virus, etc)	
<b>Ports of Communication</b> (Example: TCP port 21, UDP port 53, etc)	
<b>Physical Location of System (or Network)</b>	
<b>Attempted Attack Vectors</b> (Describe the type of attacks attempted against the system and/or network, if known)	

Attack Source(s)	
<b>IP Address(es)</b>	
<b>Hostname(s)</b>	
<b>Ports of Communication (if known)</b> (Example: TCP port 21, UDP port 53, etc)	
<b>Any Other Relevant Information</b>	

Damage Assessment (may be estimated)	
<b>Impact of attack on Agency operations and/or services</b>	
<b>Staff time to detect, handle, and recover from the incident</b>	
<b>Costs due to information loss, downtime, or other</b>	
<b>Current System (or Network) Status</b>	