Draft
Title: Incident Response and Reporting Procedure for State Government

(Date of last revision: 10/15/01)

State Agencies shall prepare procedures for reporting security breaches and incidents. Documentation on security incidents shall be filed with the Chief Information Officer for the State of Nebraska.

Policy Category Security Breaches and Incident Reporting Policy	**Policy Standard** Incident Response and Centralized Reporting	**Rule Number**
Rule Date	**Rule Revision Date** mm/dd/yy	**Date Adopted ?** mm/dd/yy
Approval NITC (pending)	**Rule Source**	**Audit Number/ Code (?)**

Explanation / Key Points

Security is a growing problem. Effective response and collective action are required to counteract security violations and activities that lead to security breaches. Agency management, law enforcement, and others must know the extent of security problems in order to make proper decisions pertaining to policies, programs and allocation of resources. Responding to security alerts will help to preempt incidents from occurring. Quick reporting of some incidents, such as new viruses, is essential to stopping them from spreading and impacting other systems. Reporting computer crimes is the only way for law enforcement to deter and apprehend violators.

Effective response to security incidents requires quick recognition of problems and fast mobilization of skilled staff to return systems to normal. This requires prior documentation of procedures and responsibilities of everyone with a role in responding to the emergency. Continuous improvement by eliminating points of vulnerability and applying lessons learned is an essential component of incident response.

Centralized reporting serves the goal of increasing awareness of vulnerabilities and threats to state government as a whole. In particular, centralized reporting is necessary to discern patterns, identify areas of vulnerability, allocate resources, and develop statewide solutions. Centralized reporting does not substitute for

internal reporting to management, reporting to law enforcement, or mobilizing a computer security incident response team (CSiRT). Agencies should develop procedures for internal and external reporting that will meet the needs of centralized reporting with little or no additional work. The centralized reporting is designed to mesh with the postmortem analysis that should follow each incident.

The ultimate goal of security incident response and centralized reporting is to protect data and prevent obstruction of government operations.

Applicability

All non-education state agencies, boards, and commissions, which receive a direct appropriation from the Legislature or any state agency that has a direct connection to the state's network. Educational institutions and other entities are encouraged to develop their own security incident and centralized reporting procedures.

Step-by-step procedure(s)

The Incident Response and Centralized Reporting Procedure for State Government requires that the agency implement the following steps for a complete security incident handling process.

1. Establish general procedures for responding to incidents;
2. Prepare to respond to incidents;
3. Analyze all available information to characterize an intrusion;
4. Communicate with all parties that need to be made aware of an incident and its progress;
5. Collect and protect information associated with an incident;
6. Apply short-term solutions to contain an incident;
7. Eliminate all means of vulnerability pertaining to that incident;
8. Return systems to normal operation;
9. Closure: Identify and implement security lessons learned.

Step 1 should include establishing a computer security incident response team (CSIRT) that can take responsibility for managing security incidents. The CSIRT can be a virtual team that includes people with a wide range of expertise. Agencies should consider forming a CSIRT that serves multiple entities. A clear description of roles and expectations is essential.

Step 2 should include methods for placing the CSIRT on alert status and ready to take preventative measures. It should include procedures for activating the team once an incident occurs.

Step 4 includes contacting users affected by an incident, security personnel, law enforcement agencies, vendors, the CERT Coordination Center (**http://www.cert.org/**), and other CSIRTs external to the organization. It is

essential that each agency establishes and follows a single channel of communication. Multiple sources of information while the incident is underway creates confusion, interrupts the work of the response team, and increases vulnerability if the perpetrator is monitoring communications within the agency.

Step 9, "Closure" is intended to give the organization an opportunity to learn from the experience of responding to an incident. Every successful intrusion or other incident indicates potential weaknesses in systems, networks, operations, and staff preparedness. These weaknesses provide opportunities for improvement. Steps should include the following points (from CERTCC security practices, http://www.cert.org/security-improvement/practices/p052.html):

1. Hold a post mortem analysis and review meeting with all involved parties. Do this within three to five working days of completing the investigation of an intrusion. Use the attached reporting form to gather information and guide discussion.
2. Prepare a final report for senior management and the Office of the CIO. This ensures awareness of security issues. Use the attached form (or online version) to report information about the security incident to the Office of the Chief Information Officer. Incidents should be reported no later than 5 working days after returning systems to normal operation.
3. Revise security plans and procedures and user and administrator training to prevent future incidents. Include any new, improved methods resulting from lessons learned.
4. Determine whether or not to perform a new risk analysis based on the severity and impact of an intrusion.
5. Take a new inventory of your system and network assets.
6. Participate in investigation and prosecution, if applicable.

Terminology

Agency. As used here, an agency is any non-education agency, board or commission, which receives a direct appropriation from the Legislature.

Security Incident. A security incident includes, but is not limited to the following events, regardless of platform or computer environment:

1. Evidence of tampering with data;
2. Denial of service attack on the agency;
3. Web site defacement;
4. Unauthorized access or repeated attempts at unauthorized access (from either internal or external sources);
5. Social engineering incidents;
6. Virus attacks affecting servers or multiple workstations;
7. Other incidents that could undermine confidence and trust in the state's information technology systems.

Related Rules

Draft security standards for the federal Health Insurance Portability and Accountability Act (HIPAA) would establish administrative procedures to guard data integrity, confidentiality, and availability. These include security incident procedures (45 CFR Part 142.308 (a)(9):

"(9) Security incident procedures (formal documented instructions for reporting security breaches) that include all of the following implementation features:

"(i) Report procedures (documented formal mechanism employed to document security incidents).

"(ii) Response procedures (documented formal rules or instructions for actions to be taken as a result of the receipt of a security incident report)."

Attachments/ Forms

State of Nebraska
Cyber Threat and Computer Intrusion Incident Reporting Form

Point of Contact Information

Name	
Title	
Telephone/Fax Numbers	
Email	
Agency	

B. Incident Information

1. Background Information:	
a. Agency (if same as above, enter "SAME":	
b. Physical Location(s) of affected computer system/network (be specific):	
c. Date/time of the incident:	
d. Duration of the incident:	
e. Is the affected system/network critical to the agency's mission? (Yes/No)	

2. Nature of Problem (check all that apply):	
a. Intrusion	
b. System impairment/denial of access	
c. Unauthorized root access	
d. Web site defacement	
e. Compromise of system integrity	
f. Hoax	
g. Theft	
h. Damage	
i. Unknown	
j. Other (provide details in remarks)	
k. REMARKS:	

3. Has your agency experienced this problem before? (Yes/No; If yes, please explain in the remarks section.)
a. REMARKS:

4. Suspected method of intrusion/attack:	
a. Virus (provide name, if known)	
b. Vulnerable exploited (explain)	
c. Denial of Service	
d. Trojan Horse	
e. Distributed Denial of Service	
f. Trapdoor	
g. Unknown	
h. Other (Provide details in remarks)	
i. REMARKS:	

5. Suspected perpetrator(s) or possible motivation(s) of the attack:	
a. Insider/Disgruntled Employee	
b. Former employee	
c. Other (Explain remarks)	
d. Unknown	
e. REMARKS:	

6. The apparent source (IP address) of the intrusion/attack:

7. Evidence of spoofing (Yes/No/Unknown)

8. What computers/systems (hardware and software) were affected (Operating system, version):	
a. Unix	
b. OS2	
c. Linux	
d. VAX/VMS	
e. NT	

f. Windows	
g. Sun OS/Solaris	
h. Other (Please specify in remarks)	
i. REMARKS:	

9. Security Infrastructure in place. (Check all that apply)	
a. Incident/Emergency Response Team	
b. Encryption	
c. Firewall	
d. Secure Remote Access/Authorization Tools	
e. Intrusion Detection System	
f. Security Auditing Tools	
g. Banners	
h. Packet filtering	
i. Access Control Lists	
j. REMARKS:	

10. Did intrusion/attack result in a loss/compromise of sensitive or information classified as private?	
a. Yes (provide details in remarks)	
b. No	
c. Unknown	
d. REMARKS:	

11. Did the intrusion/attack result in damage to system(s) or data?	
a. Yes (provide details in remarks)	
b. No	
c. Unknown	
d. REMARKS:	

12. What actions and technical mitigation have been taken?

a. System(s) disconnected from the network?	
b. System Binaries checked?	
c. Backup of affected system(s)?	
d. Log files examined?	
e. Other (Please provide details in remarks)	
f. No action(s) taken	
g. REMARKS:	

13. Has law enforcement been notified? (Check all that apply.)	
a. Yes-local law enforcement	
b. Yes-Nebraska State Patrol	
c. Yes-FBI field office	
d. Not	
e. REMARKS:	

14. Has another agency/organization been informed as assisted with the response?	
a. Yes-Information Management Services	
b. Yes-Division of Communications	
c. Yes-CERT-CC	
d. Yes-Other (provide details in remarks)	
e. No	
f. REMARKS:	

15. Additional Remarks:

If the reported incident is a criminal matter, you may be contacted by law enforcement for additional information.

C. Closure Information (Optional, Except 9 & 10)

1. (Optional) Did your detection and response process and procedures work as intended? If not, where did they not work? Why did they not work?
REMARKS:

2. (Optional) Methods of discovery and monitoring procedures that would have improved your ability to detect an intrusion.
REMARKS:

3. (Optional) Improvements to procedures and tools that would have aided you in the response process. For example, consider using updated router and firewall filters, placement of firewalls, moving the compromised system to a new name or IP address, or moving the compromised machine's function to a more secure area of your network.
REMARKS:

4. (Optional) Improvements that would have enhanced your ability to contain an intrusion.
REMARKS:

5. (Optional) Correction procedures that would have improved your effectiveness in recovering your systems.
REMARKS:

6. (Optional) Updates to policies and procedures that would have allowed the response and recovery processes to operate more smoothly.
REMARKS:

7. (Optional) Topics for improving user and system administrator preparedness.
REMARKS:

8. (Optional) Areas for improving communication throughout the detecting and response processes.
REMARKS:

9. (Required) A description of the costs associated with an intrusion, including a monetary estimate if possible.
REMARKS:

10. (Required) Summary of post mortem efforts.
REMARKS: