

# NITC 8-401

## State of Nebraska Nebraska Information Technology Commission Standards and Guidelines

### NITC 8-401

Title	Incident Response and Reporting Standard
Category	Security Architecture
Applicability	Applies to all state government agencies, boards, and commissions, excluding higher education

#### 1. Purpose

Computer systems are subject to a wide range of mishaps; from corrupted data files, to viruses, to natural disasters. These mishaps can occur at anytime of the day or night. Many mishaps are fixed through day-to-day operating procedures, while more severe mishaps are addressed in other plans, e.g. Continuity of Operations (COOP) plans. In some cases, incident handling actions will not be performed by a single person or on a single system. Responses to an incident can range from recovering compromised systems to the collection of evidence for the purpose of criminal prosecution. Therefore, preparation and planning for incidents, and ensuring the right resources are available, are critical to an agencies ability to adequately detect, respond and recover.

A formally documented and coordinated incident response capability is necessary in order to rapidly detect incidents, minimize loss and destruction, mitigate exploited weaknesses, and restore computing services. It prepares agencies to: efficiently respond, protect systems and data, and prevent disruption of services across multiple platforms and between agencies across the State network. Incorporated within these standards are accepted best practices within the law enforcement and Information Technology (IT) security communities. These standards will facilitate cooperation and information exchange among those responsible for responding to and reporting on incidents on any State of Nebraska information system.

#### 2. Standard

It is the responsibility of all State of Nebraska agencies that support information systems to develop, disseminate, and periodically review/update a formal, documented, incident response capability that includes preparation, analysis, containment, eradication, and recovery. In addition, lessons learned from prior and ongoing incident activities should be incorporated into the incident response capability. Agency plans should cover all potential types of incidents, including but not limited to:

- Information system failures and loss of service;
- Denial of service;
- Breaches of confidentiality

In addition to plans that recover systems or services as quickly as possible, the plan should also cover:

- Analysis and identification of the cause;
- Planning and implementation of remedies to prevent recurrence, if necessary;
- Collection of audit trails and similar evidence;
- Communication with those either affected by or potentially affected by the incident; and
- Reporting the incident

##### 2.1 Incident Response Team

Agencies should identify knowledgeable staff that can rapidly respond to, manage, and support any suspected incident to minimize damage to State information system(s), network(s) and data by identifying and controlling the incident, properly preserving evidence, and reporting to appropriate entities. An agency contact list should be developed and maintained for incident response personnel, which includes the names, telephone numbers, pager numbers, mobile telephone numbers, e-mail addresses, organization names, titles, and roles and responsibilities for all key incident response resources, including but not limited to agency personnel and management, other key state agencies, vendors, and contacts.

## 2.2 Initiate an Incident Log

Documentation of information is critical in situations that may eventually involve authorities, as well as provides a historical event of the actions taken to resolve the event. Manually written incident logs are preferable since electronic logs can be altered or deleted. The minimum information that should be recorded is:

- When (date and time) and how the incident was reported, discovered or occurred;
- Who reported or discovered the incident;
- Description of the incident;
- Incident-related tasks and who performed each, and the amount of time spent on each task;
- Individuals contacted regarding the incident; and
- Information system(s), program(s) or network(s) affected.

## 2.3 Classification of Cyber Security Incidents

The agency Information Security Officer (ISO) should review the incident information to determine if an actual incident has occurred. Incidents are classified into four tiers based on the severity of the incident: Tier 1, Tier 2, Tier 3, or Tier 4.

Tier	Definition	Examples	Report to SISO (See § 4.3.)	Activate Agency IRP
1	Localized, minor incidents. Non-critical systems.	- Localized virus attacks - Sustained attempts at intrusion, scanning or pingging of state devices - Missing IT devices or equipment with storage capabilities	Report aggregate results to the SISO on a monthly basis	No
2	Incidents affecting critical systems or information; or affecting more than one agency.	- Coordinated, distributed attacks - Any attack which causes Denial of Service - Financial fraud - Unauthorized activity involving a server, host, or Confidential system (HR, Legal, Financial, etc.) - Theft of proprietary information - Internet abuses violating Federal/ State law - Theft of IT devices with storage capabilities	Report verbally to the SISO immediately for determination of escalation, and/or assistance.	Yes
3	Incidents impacting multiple agencies	- Service provider outage - Core network outage - Mainframe outage	Report verbally to the SISO immediately.	Yes
4	Governor declared emergency	- Activation of COOP Plan	No	As directed

## 2.4 Cyber Security Incidents

Each agency shall securely maintain any information collected, generated, or assessed

in the course of determining whether an incident is a potential cyber security incident warranting prosecution. Data collection shall focus on identifying who, what, when, where, and the how of an incident. Collected information shall be properly documented and safeguarded. Evidence such as system and network log files, user files, system administrator logs and notes, backup-up tapes, and intrusion detection system logs, alarms or alerts shall be securely maintained and the chain of custody preserved by:

- Ensuring the evidence has not been altered;
- Ensuring the evidence is accounted for at all times;
- Verifying the passage of evidence from one party to another is fully documented; and
- Verifying the passage of evidence from one location to another is fully documented.

If an incident is determined not to be a cyber security incident, agencies are still required to maintain any evidence and its chain of custody because future incidents may require the previously captured evidence.

#### **2.4.1 Security Incident Evidence File**

An evidence file shall be created to record and maintain an inventory of all actions taken, action timestamps and correspondence associated with a security incident.

#### **2.4.2 Notification of Personal Information Security Breach**

Agencies shall determine if the incident resulted in a breach to a system containing personal information and then notify affected individual as required by the Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006 (Neb. Rev. Stat. § 87-801, et. seq.) or other State or Federal regulatory guidelines.

#### **2.4.3 Security Incident Confidentiality**

Communication shall be on a need-to-know basis and shall be considered confidential during a security incident investigation. Incident responders are not to share any details with anyone other than the Incident Response team, agency management or the State Information Security Officer (SISO) (See Section 2.12).

### **2.5 Reporting to the State Information Security Officer**

Agencies shall report incident information to the SISO. The SISO will contact appropriate authorities in accordance with State or Federal incident reporting procedures, applicable laws, directives, policies, regulations, standards, and procedures; and to US-Cert and law enforcement, if necessary. Reporting to the SISO does not relieve agencies from other reporting requirements.

The SISO has the responsibility to inform other agencies about incidents impacting multiple agencies that may become a potential threat.

### **2.6 Escalation Process**

Agencies should periodically review the incident conditions and determine if escalation to a higher tier is appropriate. An incident may be escalated in any of the following ways:

- Determination by the Chief Information Officer or State Information Security Officer;
- Additional related events (i.e. emergence of a distributed, coordinated attack, etc.)
- Requested by agency management.

### 2.6.1 Escalation Thresholds

Agencies should consider escalating an incident when certain conditions are met. The following thresholds of incident actions are examples of when to consider incident escalation:

- Multiple machines per LAN segment showing Intrusion Prevention System signature;
- Multiple machines showing multiple Intrusion Prevention System signatures;
- One or more critical infrastructure/application showing Intrusion Prevention system signatures;
- Significant impact on bandwidth;
- When a concerted effort is shown to be attacking the network, either internally or externally;
- Any known or reported compromise of Personal Identifiable Information (PII);
- Any website defacement.
- Abnormal increases in any of the above

## 2.7 Response to Incidents

Priority in incident response is given to preventing further damage to State information systems. Therefore, the Office of the CIO reserves the right to quarantine any potentially threatening agency or system.

### 2.7.1 Incident Containment

Agencies shall identify containment strategies to control an incident's impact to compromised systems, limit the extent of the incident, prevent further damage and regain normal operations of affected systems. Agency containment measures should take into consideration available resources, the classification of an incident, agency Continuity of Operations Plans (COOP) and procedures regarding response methods. Containment measures shall also be evaluated against the potential loss or corruption of security incident evidence. Containment methods shall include as a minimum:

- Ensuring redundant systems and data have not been compromised;
- Monitoring system and network activity;
- Disabling access to compromised shared file systems;
- Disabling specific system services;
- Changing passwords or disabling accounts;
- Temporarily shutting down the compromised or at risk system; and
- Disconnecting compromised or at risk systems from the network.

### 2.7.2 Incident Eradication

Agencies shall develop and employ mitigation strategies prior to returning compromised systems to service to protect against like or similar types of incidents in the future. Mitigation strategies may include, but are not limited to:

- Changing passwords on compromised systems;
- Disabling compromised accounts;
- Identifying and removing an intruder's access method;
- Installing system patches for known weaknesses or vulnerabilities;
- Adjusting or deploying firewall or intrusion detection system technologies to detect access and intrusion methods; and
- Code changes to internal applications.

## 2.8 Recovery

Agencies shall evaluate and determine when to return compromised systems to normal operations. Access to compromised systems shall be limited to authorized personnel until the security incident has been contained and root cause mitigated. Analysis and mitigation procedures shall be completed as soon as possible, recognizing agency systems are vulnerable to other occurrences of the same type. Recovery procedures shall address:

- **Recovery Requirements.** The agency shall define and prioritize the requirements to be met before returning an affected or compromised system to normal operations. Recovery strategies may include, but are not limited to:
  - Reinstalling compromised systems from trusted backup-ups; and
  - Reinstalling system user files, startup routines, or settings from trusted versions or sources.
- **Validate Restored Systems.** Agencies shall validate the restored systems through system or application regression tests, user verification, penetration tests, and vulnerability testing and test result comparisons.
- **Increased Security Monitoring.** The agency shall heighten awareness and monitoring for a recurrence of the incident.

## 2.9 Follow-up Analysis

After an incident has been fully handled and all systems are restored to a normal mode of operation, a follow-up analysis should be performed within three to five days of recovering from the incident to discuss actions that were taken and lessons learned. Extended delays may reduce the effectiveness of relating critical information. Follow-up analysis include a review of the chronological events, identifying all containment and eradication actions taken, identification of mitigation strategies, examining the lessons learned, and assessing the incident costs. Questions to be addressed may include, but are not limited to:

- Did detection and response systems work as intended? If not, what methods would have prevented the incident?
- Are there additional procedures that would have improved the ability to detect the incident?
- What improvements to existing procedures and tools would have aided in the response process?
- What improvements would have enhanced the ability to contain the incident?
- What correction procedures would have improved the effectiveness of the recovery process?
- What updates to agency policies and procedures would have allowed the response and recovery processes to operate more smoothly?
- How could user and system administrator preparedness be improved?
- How could communication throughout the detection and response processes be improved?
- Was the incident previously identified as a potential threat?
- What was the impact in terms of financial loss, loss of public or customer trust, legal liability, or harm to public health and welfare?

Results of these questions should be documented and incorporated into existing procedures, if necessary.

## 2.10 Incident Response Training

### 2.10.1 All Users

Agencies should provide education and awareness programs for users in incident response procedures and reporting methods. The programs shall address:

- What types of events are incidents;
- Agency notification procedures; and
- Existing and emerging threats.

### **2.10.2 Agency IT Staff**

Agency staff responding to incidents are encouraged to obtain the following training, according to their roles and responsibilities:

- State and Federal security and privacy laws and procedures
- Technical training on all platforms, operating systems and applications they may be responding to.

### **2.11 Incident Response Testing**

Testing should be conducted at least annually, either in response to an identified incident or as part of a formal readiness test, using defined tests, simulated events, and exercises to determine the effectiveness of the incident response capability.

### **2.12 Release of Information**

Control of information during the course of an incident or investigation of a possible incident is very important. Only the affected agency can authorize the release of all incident information. Specific information concerning the incident, such as accounts involved, programs or system names, are not to be provided to any callers regardless of who they claim to be.

## **3. Applicability**

### **3.1 State Government Agencies**

This standard applies to all state government agencies, boards, and commissions, excluding higher education.

### **3.2 Waiver**

No waivers are allowed for this standard.

## **4. Responsibility**

### **4.1 NITC**

The NITC shall be responsible for adopting minimum technical standards, guidelines, and architectures upon recommendation by the technical panel. (Neb. Rev. Stat. § 86-516(6))

### **4.2 State of Nebraska Information Security Officer**

The SISO serves as a security advisor to all State of Nebraska agencies and shall act as the incident response coordinator for the state. In that capacity, the SISO shall perform the following functions:

- Create a statewide incident response reporting procedure and instruct agencies as to the requirements of the procedure.
- Maintain a central list of agency Information Security Officers or incident response point of contact information.
- Receive incident reports, and evaluate, verify, validate and as needed disseminate alerts to State of Nebraska agencies. Alert notification will not include the name of impacted agencies or agency specifics, unless permitted.
- Coordinate with affected agencies in determining the need to disseminate alerts to federal entities, law enforcement, and any other appropriate parties.

### 4.3 State Agencies

When a Tier 2, Tier 3, or Tier 4 incident occurs, agencies must provide a verbal report to the SISO based upon the guidelines listed in Section 2.3. A written preliminary report must be completed within two (2) working days using the Incident Reporting Form (see Attachment A). This report is to be completed by the individual handling the incident; however all people involved are responsible for providing information regarding their actions. Within ten (10) working days of the resolution of an incident, a written final report must be submitted. In cases where incident resolution is expected to take more than thirty (30) days, a weekly status report must be submitted to the SISO.

Should an incident be serious enough to warrant prosecution, law enforcement will need to demonstrate a chain of custody and provide records of actions taken; therefore a log must be kept, including recovery steps and other regular or routine work performed on the affected system(s). This log should be separate from normal system logs, since it may be used as evidence.

Agencies are responsible for submitting a monthly report (see Attachment B) that document the aggregate number of various types of incidents.

Agencies are responsible for training personnel in incident response capabilities according to their roles and responsibilities.

Agencies that support information systems shall provide a support resource, i.e. a Help Desk, which serves as the primary contact to report incidents.

#### 4.3.1 Agency Incident Response Contacts

Agencies are responsible for providing a primary and secondary point of contact to act as a liaison with the SISO. The agency point of contact can be the agency Information Security Officer (ISO) or some other designee. See Information Security Policy, Appendix B for Roles and Responsibilities of the (ISO).

### 4.4 Users

All information system(s) users are responsible for understanding their role and complying with agency incident handling procedures. Users must immediately report suspicious activities to their manager and/or agency or State of Nebraska HelpDesk and fully cooperate with personnel tasked with resolving the incident.

## 5. Related Documents

5.1 [NITC 8-RD-01](#): Security Officer Instruction Guide

5.2 [NITC 8-101](#): Information Security Policy

## 6. References

6.1 **National Institute Standards and Technology (NIST) Special Publication, 800-61**, "Computer Security Incident handling Guide." (<http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf>).

[Attachment A](#): Incident Response Form (Word Document)

[Attachment B](#): [Link to be added]

[Attachment C](#): Incident Handling Lifecycle

-----

VERSION DATE: February 22, 2008

HISTORY: Original versions of related documents adopted on January 23, 2001 and June 18, 2002. Contact information revised on August 10, 2006. Revised version adopted on March 4, 2008. Contact information in Attachment A revised on January 23, 2009.

PDF FORMAT: <http://nitc.ne.gov/standards/8-401.pdf>

-----