DHHS Information Technology (IT) Incident Management Standard

Issue Date: October 1, 2013
Effective Date: October 1, 2013
Revised Date:

Number: DHHS-2013-001-E

1.0 Purpose and Objectives

Computer systems are subject to a wide range of mishaps; from corrupted data files, to viruses, to natural disasters. These mishaps can occur at any time of the day or night. Many mishaps are fixed through day-to-day operating procedures, while more severe mishaps are addressed in other ways (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 agency's 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 Nebraska's Department of Health and Human Services (DHHS) to efficiently respond, protect systems and data, and prevent disruption of services across multiple platforms and between all agencies across the State and DHHS network.

The DHHS IT Incident Management Standard and Procedures includes multiple processes throughout DHHS and Information Systems and Technology (IS&T). It includes a number of operational and technical components which provide the necessary functions in order to support all the fundamental steps within the Incident Management Life Cycle - including Preparation, Identification, Containment, Communication, Eradication, Recovery, and Root Cause/Remediation. It is also a necessary component to Information Technology strategy and long term planning. It is required by DHHS policy, as well as the Federal Information Security Management Act (FISMA), Health Insurance Portability and Accountability Act (HIPAA), and Internal Revenue Service (IRS) regulations. DHHS security policy requires the establishment and maintenance of a computer security incident response capability that is in effect 24x7.

This document identifies key steps for promptly reporting security incidents and establishes formal reporting requirements for all such instances to the DHHS Information Security Officer (ISO), DHHS Privacy Officer, State officials, and DHHS customers. All security incident reports are to contain the facts and information needed to make informed management decisions and to assist in coordinating and managing the resolution(s).

2.0 Scope and Responsibilities

A security incident is any adverse event whereby some aspect of the DHHS infrastructure is threatened (e.g., personal violation, loss of data confidentiality, disruption of data integrity, denial of service, security breach). It is important to note that even if there is no evidence of information being accessed by unauthorized personnel, exposing sensitive information in an unsecure manner is considered a security breach. For example, any email that is sent outside the secured DHHS network that contains protected health information (PHI), personally identifiable information (PII), or federal tax information (FTI) and is not encrypted IS a security breach and MUST be reported as such. All security incidents MUST be reported to the DHHS ISO or DHHS Help Desk **IMMEDIATELY**.

Key roles and responsibilities for DHHS personnel include the following:

All DHHS Personnel

- Report security incidents to the ISO or the DHHS Help Desk immediately.
- Assist ISO and IT Team with remediation and reporting.
- Follow instruction from ISO or IS&T before taking action.
- Do NOT communicate information regarding the incident unless authorized.

Senior DHHS Management

- Coordinate with ISO, Legal, and Privacy Office and communicate reportable breaches of PHI, PII, and FTI as required by regulation within one (1) hour of awareness.
- Provide support and resources necessary to contain and remediate incidents.
- Provide command and control of the situation.

DHHS Legal and Privacy Office

- Work with ISO to triage and assess reportable conditions.
- Craft communications for customers, government officials and the public in the event of a reportable breach.
- Breaches of PHI and PII must be reported within required time frames.
- Ensure all third-party agreements have requirements to comply with DHHS Incident Management requirements.

DHHS ISO

- Assembles and engages the DHHS Incident Response Team.
- Coordinates the management of security incidents and follow-up activity.
- Advises DHHS Management and works with IS&T Management to perform analysis and triage of incident impact and reportable conditions.
- Coordinate communication content and plans with DHHS Management.
- Work with IS&T teams to prepare remediation and countermeasures.
- Finalize Security Incident Reports .

- Reviews requests for release of security incident information.
- Determines follow-up activity and conducts root cause analysis, long term mitigation, and awareness.
- Perform review and inspection of business partners and their ability to meet requirements with this standard.
- Perform education and training of this standard to all applicable DHHS personnel
- Test the Incident Management Process annually.

DHHS CIO

- Review all requests for the release of security incident information and make determinations with regard to its release.
- Issue an order of action if security incident is not controlled in a timely manner.
- Determine impact and priority of security incidents.
- Provide command, control, and oversight of information security incident triage, containment, remediation, and communication activity.

DHHS Incident Response Team

DHHS shall identify key personnel who will serve as members of the DHHS Incident Response Team. This team will be made up of knowledgeable staff that can rapidly respond to, manage, and support any suspected incident to minimize damage to DHHS information system(s), network(s) and data by identifying and controlling the incident, properly preserving evidence, and reporting to appropriate entities. DHHS ISO will maintain a contact list which includes the names, telephone numbers, pager numbers, mobile telephone numbers, email 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.

3.0 Procedures

Completed Security Incident Report information is classified as Highly Restricted Information. Sharing or distribution of the information will be limited to only those individuals with a valid need-to-know. The Chief Information Officer (CIO), with consultation from the DHHS ISO and IS&T management, will review all requests for the release of security incident information and make determinations with regard to its release, ensuring that it is consistent with applicable policies, regulations, and external customer requirements. Overall questions regarding this procedure should be directed to the DHHS ISO.

3.1 Incident Components

The four major components of our Security Incident Response procedure include:

- Incident Identification*:* Formal acknowledgement that a security incident has occurred.
- Incident Procedure*:* The actions taken to resolve the security incident.

- Incident Analysis*:* The analysis of how the security incident happened, the assessment of the security incident.
- Incident Recovery: The activity necessary to return to normal operations and implement long-term corrective actions to minimize the probability of the incident recurrence.

The goal of this procedure is to respond to each incident effectively and as close to real time as possible to protect DHHS information assets.

3.1.1 Incident Identification

Depending on who received the initial notification of an incident, triage shall be conducted by the DHHS ISO, DHHS Help Desk, or IS&T Management to understand the impact of the incident and initiate appropriate action. Once an incident has been identified and reported the ISO will assume oversight of the incident response and will continually assess the incident conditions and determine if escalation of response actions is appropriate. Prevention of damage is given priority over forensics of incident source. Therefore, the DHHS ISO and DHHS CIO reserve the right to quarantine any potentially threatening system and terminate any threatening activity using all means necessary. DHHS acknowledges and will comply with NITC 8-401 Incident Response and Reporting Procedure for State Government Standard.

3.1.2 Incident Procedure

At a minimum, DHHS internal procedures require, first and foremost, prevention of damage from the incident over forensics. This means that the first priority is to shut off or terminate any potential threat. It is strongly desired to perform this action in a manner that allows for preservation of evidence, but if there is ANY doubt, all DHHS personnel, whether employees or contractors, are required to disable the threat immediately. Following the assessment and termination of the threat, the next priority is containment followed by recovery actions, damage determination, report documentation, lessons learned, and identification of corrective actions. Distribution and/or notification will include coordination of the ISO, IS&T CIO, Legal, and the Privacy Officer. These are the only parties who will communicate to customers or Senior Leadership of DHHS. All outsourced support, including any Information Technology Support, will communicate with the parties necessary for responding to the incident, and the ISO or IS&T management only.

1. As soon as an incident is detected, personnel qualified and designated to respond shall be notified to take immediate action, determine incident impact, file a ticket, or prepare a report.
   a. All security incidents are initially reported to and tracked by the ISO. Any DHHS employee or contractor who observe, experience, or are notified of a

security incident, should immediately report the situation to the ISO or the DHHS Help Desk. All contracted support personnel are required to notify DHHS ISO *immediately* of any suspected security incident or breach.

b. If the incident appears to have ANY client information compromised, including any PHI, PII, or FTI, immediate notification to the DHHS ISO, Legal, Privacy Officer, or DHHS CIO is REQUIRED. The Privacy Officer or DHHS CIO will notify Senior State officials and will determine the level of contact with DHHS customers and government agencies. DHHS Senior Management or designates will oversee and coordinate all communication actions.

c. Incident triage to establish the impact level will be conducted by the DHHS Help Desk, DHHS ISO, or IS&T Management. Corresponding notifications of officials and Incident Response Team will be completed.

d. Reportable conditions, such as the breach of PII, PHI, or FTI, require notification within specific timeframes (as defined in state and federal regulations) of DHHS becoming aware of an incident.

e. The DHHS ISO will issue the order of action, if a security incident is not controlled in a timely manner *(typically 12 hours)*.

2. Upon confirmation, the security incident response actions and remediation will be immediately implemented and documented by the DHHS ISO. Depending on the nature of the security incident, a post-mortem meeting may be conducted.

3. All incidents except those classified as have a low impact are required to have an incident report completed. Documentation of information is critical in situations that may eventually involve authorities as well as provides documentation of the actions taken to resolve the event. A copy of the incident report form is available from the ISO.

3.1.3 Incident Analysis

A damage analysis of security incidents is to be initiated immediately after assessment by the DHHS ISO, IS&T Management and their engineering and security teams as required. The ISO and IS&T will determine if the incident impacts organizations outside of the DHHS internal network. All compromised systems will be disconnected from external communications immediately upon discovery. DHHS Senior Management will be notified of analysis results and client impact immediately upon discovery, and shall be kept abreast of all analysis findings, impact assessments, and remediation progress.

In the event of a discovery of a breach of system security protections, an internal security investigation must be properly performed. The chain of custody steps that should be taken in the event of a security breach are as follows:

a. If the system can be taken off the network, do it. Pull the network cable. If possible, do NOT shut down the system! Do not log in or change passwords if possible. Do NOT turn off the system – unless that is the only way to stop the threat.

b. If the system cannot be taken off the network, take pictures and screenshots.

c. Notify the DHHS ISO immediately after initial steps, but NO LATER than 30 minutes after becoming aware of the possible incident.

d. Image the drive before investigating (i.e., opening files, deleting, rebooting).

e. Dump memory contents to a file.

f. Log all steps.

g. Label all evidence.

h. Present an affidavit to maintain the chain of custody.

Additional **virtual considerations** to meet chain of custody requirements that may be required:

a. Instruct IS&T to suspend any VM, do not disable Hypervisor port or shutdown VM. Powering off the VM could delete copies of the physical RAM and sensitive information making it impossible to determine which blocks were affected.

b. Create a non-repudiation signature of the VM by hashing, and password protecting any saved files or folders.

c. Create a virtual bridge, and create/move to containment VLAN and set security rules. Move the compromised VM to a containment or secured VLAN.

   Or

   Move the signed instance of the VM to a secured removable storage device which can be presented to the authorities.

d. Collect ESX, VM, Hypervisor, VCenter and applicable tool logs to determine impact and breach tracking.

In the event data destruction is required, personnel are required to follow the DHHS Policy on Media Sanitation, and sanitize information systems' media prior to media retirement using approved sanitization or degaussing. This activity will be tracked and recorded (see NIST 800-88 for guidance).

3.1.4 Incident Recovery

The DHHS Incident Response team working with application and data owners 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 DHHS 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.
- Validating Restored Systems. DHHS shall validate the restored systems through system or application regression tests, user verification, penetration tests, and vulnerability testing and test result comparisons.
- Increasing Security Monitoring. DHHS shall heighten awareness and monitoring for a recurrence of the incident.

4.0 Incident Management Training and Testing

DHHS shall provide training on incident recognition and reporting requirements to all staff and contractors. More in depth training and awareness will be given to all applicable staff in incident response and recovery procedures and reporting methods. The DHHS ISO shall provide annual training and simulated incident response and recovery testing for the DHHS Security Incident Response team. The DHHS ISO and DHHS Incident Response Team shall also receive annual education and awareness of the various laws and regulations related to privacy and reporting of breaches of PHI, PII or FTI.

5.0 Revision History

Legal Review – 09-30-2013
Policy Approved – 09-30-2013

Signature:

Date: 9/30/2013

Eric Henrichsen
Information System & Technology Administrator
Nebraska Department of Health & Human Services