

## **DHHS POLICIES AND PROCEDURES**

---

<b>Section VIII:</b>	<b>Privacy and Security</b>
<b>Title:</b>	<b>Security Manual</b>
<b>Chapter:</b>	<b>Information Incident Management Policy</b>
<b>Current Effective Date:</b>	<b>6/15/05</b>
<b>Revision History:</b>	
<b>Original Effective Date:</b>	

---

### **Purpose**

To define the processes and procedures that will enable the Department of Health and Human Services (DHHS) Divisions/Offices to identify and respond to a broad range of information security incidents. This policy is based upon the Information Technology Services (ITS) Incident Management Policy and the Incident Response Standard and other state/federal requirements.

### **Policy**

DHHS shall rapidly identify, report, manage, mitigate and resolve DHHS information security incidents.

### **Roles and Responsibilities**

The primary responsibilities associated with incident management are to identify and respond to suspected or known security incidents, contain or limit the exposure to loss, and mitigate (to the extent practical) the harmful effects of security incidents.

The DHHS Divisions/Offices will manage incidents at the facility level and will alert the DHHS Privacy and Security Office to potential department-wide threats. Where facilities are leased or ITS support is provided by an affiliate(s), a DHHS Division/Office security representative shall be assigned to facilitate the handling of security incidents. The nature of the incident may require the assignment of staff from other divisions/offices.

In all cases, division/office management shall be informed of the incident and the steps recommended or taken to mitigate the incident.

### **Implementation**

The DHHS Privacy and Security Office (PSO) shall develop, maintain and implement an incident management and response plan that addresses information technology security incidents. The following paragraphs specify the incident management plan requirements.

These requirements shall be in compliance with relevant federal/state and DHHS policies and standards.

1. *Incident Management Training:* The DHHS PSO shall provide incident management training to the DHHS Divisions/Offices on how to identify and report security incidents.
2. *Identifying and Prioritizing Types of Incidents:* The DHHS PSO will develop and maintain guidelines for identifying and prioritizing security incidents.

DHHS Divisions/Offices or their affiliated staff designated by agreement or assignment shall evaluate the potential for the occurrence of certain types of incidents. All security incidents shall be classified by severity level and type.

The following five (5) event severity levels as defined in the ITS Incident Response Standard shall be used for classification purposes. In addition, each incident shall be identified as to type: email, hacking, virus/worm, inappropriate use, social engineering and other.

3. *Incident Monitoring:* The DHHS PSO shall develop and maintain guidelines on how to monitor for security incidents.

The DHHS Divisions/Offices or their affiliated staff designated by agreement or assignment, as part of their risk management program, shall continuously monitor for security incidents (both physical and ITS - related incidents) according to the guidelines listed above.

4. *Incident Detection:* The DHHS PSO shall develop and maintain enterprise-wide procedures for collecting, analyzing and reporting data.

The integrity of all data relating to criminal acts must be preserved as possible evidence and will be collected using generally accepted forensic procedures. The forensic procedures to be followed will be developed and disseminated by the DHHS PSO.

5. *Incident Reporting:* The DHHS PSO shall define the basic procedure to be followed for reporting incidents. The procedure shall be expanded upon by the DHHS Divisions/Offices as necessary to include the internal communications and escalation procedures that will be used.

Security incidents classified as level 3, 4, or 5 shall be reported to the DHHS PSO and the division/office information security official within a period of 24 hours from the time the incident was discovered. The DHHS PSO is responsible for reporting the incidents to ITS and the DHHS Assistant Secretary for the OPP and Compliance within 24 hours of receiving the report. The DHHS Assistant Secretary for OPP and Compliance will be responsible for letting appropriate departmental staff know about

the issue. The division should not report directly to ITS, as it could result in duplicate incidents being reported. The incident shall be entered by the division/office staff in accordance with division/office procedures at the following site: [http://www.security.dhhs.state.nc.us/incident\\_report.aspx](http://www.security.dhhs.state.nc.us/incident_report.aspx). A manual form may be completed and forwarded to the division/office information security official for processing. An incident reporting template is located at the above referenced web site.

Reporting of security instances classified as level 2 or greater should be reported, at a minimum, to the division/office security official. Division/office specific procedures may require all levels of security incidents to be reported to the DHHS PSO. If there is a question regarding classification level, the division/office security official should consult with the DHHS PSO.

6. *Security Incident Response Team (SIRT)*: The DHHS PSO shall establish and utilize an SIRT. The PSO will work with the DHHS Divisions/Offices to develop a cross-functional incident response team that will handle a variety of incidents. The roles and responsibilities of the team members will be clearly defined.

The SIRT shall be adequately staffed and trained to handle the incident(s). Since incidents may be far-reaching, requiring expertise or authority that does not reside within a division/office, the SIRT may include outsourced vendors, internal and external entities, as well as other key facility/agency personnel.

7. *Organization Protocols*: Security incidents may occur across network boundaries. The DHHS PSO shall define the protocols for handling these incidents and the contacts between DHHS Divisions/Offices, state agencies and outsourced entities.
8. *Impact Assessment*: The DHHS PSO shall evaluate the impact of security incidents. Assessments may be required at various stages of the incident life cycle to assist management in deploying the proper risk management strategy.
9. *Incident Handling and Escalation Procedures*: The DHHS PSO shall develop and maintain the primary procedures for handling the containment, eradication and recovery aspects of incidents and the guidelines for development of an escalation procedure. The DHHS Divisions/Offices shall develop escalation procedures that are tailored to their individual circumstances.
10. *Documentation*: All security incidents shall be thoroughly documented by the DHHS Divisions/Offices with as much detail as possible to describe the incident, time discovered and impacted area for subsequent investigation. The incident report shall indicate who was notified and what actions were taken. The DHHS PSO may be called on to assist in the documentation process.
11. *Record Retention*: DHHS Divisions/Offices shall maintain the incident logs and corresponding documentation for a minimum of one (1) year following the discovery

of an incident or until an investigation is completed. Incident logs should be stored in a secure location.

12. *Post-Incident Analysis:* The post-mortem analysis provides feedback to improve the existing process and its related procedures. Following actions taken to resolve each security incident, an analysis shall be performed by the DHHS PSO and the impacted division or office, with assistance of their affiliated staff designated by agreement or assignment, to evaluate the procedures taken and what further steps could have been taken to minimize the impact of the incident.
13. *Emergency Planning:* If an incident occurs that impacts the safety of citizens, personnel, DHHS facilities or results in a situation where agency services are interrupted for an extended period of time, the incident may be declared an emergency. The DHHS PSO shall work with the DHHS Disaster Response Team to provide guidelines regarding the criteria for identifying an emergency and notification procedures. The DHHS Divisions/Offices shall develop the appropriate procedures for identifying and declaring emergencies using the established DHHS Business Continuity and Disaster Recovery Policy.
14. *Media Relations:* Serious security incidents that are likely to result in media attention shall be reported immediately to the DHHS Department of Public Affairs Office.

## **Enforcement**

*For enforcement questions or clarification on any of the information contained in this policy, please contact DHHS Security Officer ([DHHS.Security@ncmail.net](mailto:DHHS.Security@ncmail.net)). For general questions about department-wide policies and procedures, contact the [DHHS Policy Coordinator](#)*

## **Exceptions**

Any exceptions to this policy will require written authorization. Exceptions granted will be issued a policy waiver for a defined period of time. Requests for exceptions to this policy should be addressed to the Director of the Division of Information Resource Management (DIRM). The waiver request will be processed in accordance with the DHHS [ITS Waiver and Appeals Policy](#).