

DHHS POLICIES AND PROCEDURES

| | |
|---------------------------------|---|
| Section VIII: | Privacy and Security |
| Title: | Security Manual |
| Chapter: | Information Security Management Policy |
| Current Effective Date: | 6/15/05 |
| Revision History: | |
| Original Effective Date: | |

Purpose

To define an information security management infrastructure that will adequately protect the Department of Health and Human Services (DHHS) information, assets, and personnel and ensure compliance with federal and state regulations.

Policy

This policy defines the security management requirements for the DHHS Privacy and Security Office (PSO) and the DHHS Divisions/Offices. Information security management shall include but not be limited to the following areas:

1. Security budgeting and staffing;
2. Information security governance and organization of the security program, including roles and responsibilities;
3. Risk management programs;
4. Information security programs;
5. Security compliance;
6. Incident management;
7. Physical and environmental security;
8. Business continuity and disaster recovery;
9. Security training and awareness program;
10. Information Technology Services (ITS) Contract Administration and oversight; and
11. DHHS Security Work Group Support.

Roles and Responsibilities

DHHS PSO shall implement and maintain a comprehensive information security program that includes security management processes and procedures. The DHHS PSO will establish and maintain the framework to ensure that information security strategies within the DHHS Divisions/Offices are aligned with the DHHS mission and objectives and comply with the applicable federal and state laws.

DHHS Divisions/Offices shall ensure that all members of the workforce are trained in security matters. The divisions/offices shall develop the specific security procedures to address their specific circumstances, as required.

Implementation

Policy implementation shall be based upon the use of management-approved security standards and industry best practices (see references). The following paragraphs specify the requirements for information security management:

1. **Security Budget and Staffing**

The DHHS PSO shall provide assistance with the DHHS Divisions/Offices in ensuring adequate budget and staffing levels for information security. The PSO will regularly review budgets and staffing levels and make recommendations.

2. **Information Security Programs**

The DHHS PSO shall develop and implement a comprehensive Information Security Program (ISP) to meet the business, operational, regulatory, and programmatic requirements of DHHS. The DHHS Divisions/Offices or their designated affiliates shall:

- Ensure that information resources are properly managed;
- Determine the sensitivity and criticality of all data used;
- Implement data classification and control procedures in the work environment;
- Create and maintain information security plans;
- Develop information security control baselines for network, application or information systems in order to objectively evaluate division/office security;
- Develop, maintain and implement specific security policies, procedures and guidelines to supplement those of the PSO, as required, to meet their requirements;
- Follow the documentation review processes/procedures as defined by the PSO;
- Implement a change management system with document version control;
- Promote data stewardship and individual accountability among business process owners, data owners, managers and other stakeholders to manage information security risks;
- Ensure that all staff receive the security awareness training for their workforce provided by the PSO;
- Implement the risk management program for information systems developed by the PSO;
- Plan for business continuity and disaster recovery under the leadership of and following the guidelines and procedures of the PSO; and
- Implement the incident management and reporting capability.

3. **Information Security Governance**

The DHHS PSO shall:

- Provide security policies, standards and implementation guidelines to support information security governance;
- Review all security solutions prior to implementation and create a security waiver process for the DHHS Divisions/Offices;
- Develop and maintain an information security program that adequately supports the mission and objectives of DHHS;
- Develop and maintain information security strategies in support of the overall DHHS mission statement that address changes to technology, business requirements, and state and federal regulations;
- Obtain DHHS senior management commitment and support for information security throughout the organization;
- Ensure that definitions of security roles and responsibilities throughout the organization include information security governance activities;
- Establish reporting and communication channels that support information security governance activities;
- Establish and maintain security policies that support DHHS mission goals and objectives;
- Provide an information assurance framework for availability; and
- Audit all critical DHHS applications and systems on a regular basis.

4. **Risk Management Program**

The DHHS PSO shall develop a risk management standard and implementation guidelines for the DHHS Divisions/Offices (See DHHS Risk Management Policy).

The DHHS Divisions/Offices shall:

- Implement a systematic, analytical and continuous risk management program for information systems;
- Ensure that risk identification, analysis and mitigation activities are performed;
- Ensure that risk assessments are performed periodically to evaluate effectiveness of existing controls;
- Define strategies and mitigate risks to acceptable levels for the division; and
- Report significant changes in risk levels including threats and vulnerabilities to appropriate levels of management on both a periodic and an event-driven basis.

5. **Security Compliance**

The DHHS PSO shall:

- Develop and maintain a compliance management standard and implementation guidelines for the DHHS Divisions/Offices;

- Define the metrics to be used to measure, monitor and report on the effectiveness of information security controls and compliance with DHHS information security policies; and
- Reinforce security practices by providing security and awareness training.

The DHHS Divisions/Offices shall:

Ensure that the organizational, administrative, physical, and technical procedures for information systems comply with DHHS information security policies;

- Ensure that services provided by third parties, including outsourced providers, are consistent with established information security policies;
- Use the metrics defined by the PSO to measure, monitor and report on the effectiveness of information security controls and compliance with DHHS information security policies;
- Ensure that information security standards are not compromised throughout the change management process; and
- Ensure that noncompliance issues and other variances are resolved in a timely manner.

6. **Incident Management and Response**

The DHHS PSO shall develop and maintain an incident management standard and implementation guidelines for the DHHS Divisions/Offices and processes for detecting, identifying, analyzing, and reporting security-related events. Further specification are detailed in the DHHS Information Incident Management Policy.

The DHHS Divisions/Offices shall:

- Establish, maintain and implement procedures for documenting incidents as a basis for subsequent investigation; and
- Manage post-incident reviews (“lessons learned”) and document incident causes and recommended corrective actions, in consultation with the PSO.

7. **Physical and Environmental Security**

The DHHS PSO , in collaboration with Divisions/Offices, shall develop and maintain Physical and Environmental Security IT standards and guidelines for all DHHS facilities. The DHHS Divisions/Offices shall implement physical security policies and develop, maintain and implement procedures. Further specifications are detailed in the DHHS Physical and Environmental Security Policy.

8. **Business Continuity and Disaster Recovery**

The DHHS PSO shall develop and maintain BCP/DR standards and implementation guidelines for the DHHS Divisions/Offices. Further specifications are detailed in the DHHS Business Continuity and Disaster Recovery Policy.

The DHHS Divisions/Offices shall:

- Establish a business/IT recovery team;
- Develop and maintain emergency response, communication, and recovery procedures;
- Provide periodic testing of the response and recovery plans where appropriate, with assistance from the PSO, as necessary; and
- Evaluate the execution of response and recovery plans and provide feedback for improvement.

9. **Security Awareness and Training Program**

The DHHS PSO shall implement a security awareness and training program for DHHS. The PSO shall facilitate the training of the designated Information Security Officials (ISOs) of the DHHS Divisions/Offices. General security training will be provided as resources are available. The DHHS Divisions/Offices shall ensure that all personnel participate in the security awareness program and that other IT security training is provided in accordance to meet the requirements of the security classification of their job functions. Further specifications are detailed in the DHHS ITS Security Training and Awareness Policy.

10. **Contract Administration and Oversight**

The DHHS PSO shall develop and maintain required security guidelines for use in writing, developing and effectively managing outsourced Information Systems (IT) contracts. Further specifications are detailed in the DHHS Information Technology Contract Policy.

DHHS Divisions/Offices shall:

- Manage outsourced ITS contracts (via a service-level agreement); and
- Provide oversight over ITS contracts to ensure compliance with ITS security policies.

11. **DHHS Security Work Group**

The DHHS Security Work Group (SWG) shall:

- Assist the DHHS PSO in the development and maintenance of DHHS enterprise-wide security policies and procedures;
- Serve as a primary means of communication on security-related matters between the PSO and division/office management; and
- Review security policy revisions proposed by the PSO and provide division/office input.

Further specifications regarding the SWG are detailed in the DHHS Security

Organization Policy.

Enforcement

For enforcement questions or clarification on any of the information contained in this policy, please contact DHHS Security Officer (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](#).