

## **DHHS POLICIES AND PROCEDURES**

---

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

---

### **Purpose**

To implement a risk management methodology that will enable the Department of Health and Human Services (DHHS) Divisions/Offices to manage risks. Risk management includes the identification, evaluation, mitigation, and monitoring of risks related to the information technology infrastructure, the information/data, the business conducted by DHHS and the physical security to protect Information Technology Systems (ITS) assets.

### **Policy**

DHHS shall implement an enterprise-wide risk management program that enables the organization to assess and keep risks at an acceptable level.

### **Roles and Responsibilities**

The DHHS Privacy and Security Office (PSO) shall develop a risk management program that will include the following:

1. Methodology for implementing risk management including identification and analysis of risks in the workplace.
2. Enterprise-wide procedures for assessing risks and threats, and for mitigation planning.
3. Mechanisms for tracking and reporting risk.
4. Development of guidelines for Business Continuity Risk Management and Security Risk Management.
5. Risk management training for the workforce.
6. Tools and implementation support for the DHHS Divisions/Offices.

The DHHS Divisions/Offices shall implement the enterprise-wide risk management program.

## Implementation

Policy implementation shall be based upon the use of management-approved security standards and industry best practices as outlined by the DHHS PSO. The following sections specify requirements for implementing the risk management program.

1. Risk Management Framework (*The DHHS PSO shall define a risk management framework*). This framework will contain the following components:
  - A. Distribute the DHHS risk management policy to the DHHS workforce and educate the workforce on that policy; include risk management in the security education for security officials.
  - B. Identify sensitive information.
  - C. Identify main stakeholders.
  - D. Establish and define approaches to be used to identify, assess, report, and mitigate risks. This component includes the identification of federal, state and local regulatory or legal requirements that address the confidentiality, integrity and availability of information used to provide DHHS services.
  - E. Assign responsibilities for managing risk and reporting authority to senior management. Priority shall be given to risks that affect core business functions and have impact on multiple divisions/offices.
  - F. Identify any due diligence requirements for agency functions or services.
  - G. Document audit trails of decisions to ensure that risk management reflects current good practice.
  - H. Provide a mechanism for tracking and reporting risks.
  
2. Identify the risk to personal property and information assets (*The DHHS PSO shall work with each DHHS Division/Office in the following manner*):
  - A. Identify assets at risk. Consider threats, vulnerabilities and potential impact. Risk identification of personnel, information systems, facilities, and networks shall:
    1. Identify the division/office mission, location, and size.
    2. Establish and maintain an inventory of each information system, including the purpose of the system, hardware, software, system interfaces, users, present system security controls, information system criticality, and data sensitivity.
    3. Identify and assess impact of relevant regulations.
    4. Identify system threats in the environment.
    5. Identify system vulnerabilities that threats could attack
    6. Identify current security controls.
    7. Identify current security gaps (inherent and residual).
  
  - B. Aim to identify the 20% of risks that would have 80% of the potential impact.

- C. Ensure that everyone involved has an understanding of the mission, aims, objectives, and plans for delivery.
  - D. Assure realistic plans for sharing risk impact, while recognizing that customers' and providers' perspectives on risk will not be the same.
3. Identify workforce members responsible for managing risk. (*The DHHS Divisions/Offices shall perform the following activities*):
- A. Allocate responsibility for managing key risks.
  - B. Ensure that every risk has at least one owner; there may be separate owners for the actions to mitigate the risks.
  - C. Ensure that anyone allocated ownership has the authority to take on the responsibility and that they are aware that they are the designated owner.
  - D. Adopt the mechanism provided by the DHHS PSO for tracking and reporting issues.
  - E. Develop the responses or controls necessary to mitigate identified and reported risks, assisted by the DHHS PSO as necessary.
4. Risk Assessment (*The DHHS PSO shall provide the DHHS Divisions/Offices with tools to evaluate risk and guidelines for bringing all identified risks to an acceptable level. The DHHS Divisions/Offices shall perform the following activities*):
- A. Assess the probability of risks occurring and their potential impact using quantitative or qualitative analysis.
  - B. Identify all sensitive information, the mechanism used to protect that information and the potential for fraud or misuse.
  - C. Identify essential access control mechanisms used for requests, authorization, and access approval in support of critical DHHS functions and services.
  - D. Identify the risks associated with all critical processes in the workflow.
  - E. Identify all security controls currently implemented to mitigate risk.
  - F. Provide an analysis of risks. This analysis shall include an estimation of the probability, impact, and timeframe of the risks, classification into sets of related risks, and prioritization of risks relative to each other.
5. The DHHS Divisions/Offices shall identify suitable responses to risk by addressing each risk as appropriate:
- A. Risk reduction – Implement measures to alter or improve the risk position of an asset throughout the organization.
  - B. Risk transference – Assign or transfer the potential cost of the loss to another party, (i.e., insurance company).
  - C. Risk acceptance – Accept the level of loss that will occur and be prepared to absorb that loss.

## 6. Risk Mitigation

- A. The DHHS Divisions/Offices shall implement safeguards to mitigate risk and monitor their effectiveness. The DHHS Divisions/Offices shall provide mitigation planning: decisions and actions that will reduce the impact of risks, limit the probability of their occurrence, or improve the response to a risk occurrence. For important risks, mitigation plans shall be developed.

*Risk Management (DHHS Divisions/Offices shall embed the risk management procedures in the organization and on a regular basis review risk procedure processes. The following activities shall be included):*

1. Ensure that risk management is an intrinsic part of DHHS operations and that risk management is reflected in daily activities and decisions.
2. Keep risk management policies and procedures current.
3. Monitor and review risks.
4. Perform an analysis to evaluate the actions taken and to determine what further steps could be planned to minimize risk impact.
5. Compile and report on status of information about risks and mitigation plans, following the mechanism for tracking and controlling risks provided by the DHHS PSO.
6. Respond to changes in risks and take corrective action as needed.

## 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](#).