

## **DHHS POLICIES AND PROCEDURES**

---

<b>Section VIII:</b>	<b>Privacy and Security</b>
<b>Title:</b>	<b>Security Manual</b>
<b>Chapter:</b>	<b>Data Classification, Labeling and Access Control Policy</b>
<b>Current Effective Date:</b>	<b>6/15/05</b>
<b>Revision History:</b>	
<b>Original Effective Date:</b>	

---

### **Purpose**

The purpose of this document is to ensure that all the Department of Health and Human Services (DHHS) data are evaluated, properly classified and labeled and that the appropriate access controls are implemented to protect that data.

### **Policy**

DHHS shall establish and maintain an enterprise-wide data classification mechanism that includes the determination of sensitivity, labeling and access control. Data classification of DHHS applications or systems is necessary to ensure the confidentiality, integrity and availability of the data and application. The level of security controls implemented shall be commensurate with the classification of sensitivity of the information and the risk and magnitude of loss or harm that could result from improper operation. The assigned security classifications shall be maintained in a central DHHS Information Technology Services (ITS) Resource Inventory.

### **Roles and Responsibilities**

The DHHS Privacy and Security Office (PSO) shall be responsible for providing data classification and labeling standards, enterprise-wide control procedures, and guidelines.

DHHS divisions/offices shall be responsible for implementing data classification, labeling, and control procedures. The classification and assignment of security levels will be maintained on the DHHS ITS Resource Inventory. The DHHS Divisions/Offices shall also be responsible for reviewing and updating the inventory and submitting updated information in a timely manner.

The Division of Information Resource Management (DIRM) shall establish and maintain the DHHS ITS Resource Inventory.

## Implementation

Policy implementation shall comply with management approved standards, procedures and best practices. The following classifications shall be assigned and maintained on DHHS ITS Resource Inventory.

The determination or assignment of security classifications to information contained in computerized business applications in DHHS provides a framework to establish the criticality of the applications. The system owner or their affiliated staff, shall determine the classification of data confidentiality, availability risk and integrity. The overall security level for an application is the highest of the three classification assessments (confidentiality, availability and integrity).

### 1. Determination of Data Confidentiality

A process and guidelines shall be developed and maintained by the DHHS PSO, with consultation from other responsible divisions/offices, that will enable the system owner, data custodian and other key individuals to make decisions regarding the confidentiality of data. This classification will establish the general requirements for the implementation of security controls. The determination of sensitivity will be documented and maintained on file with the system owner. The three (3) general categories are: Confidential (sensitive), Public (non-sensitive) and Internal Use Only.

- Confidential – Assign the confidential level to applications with data that (1) state or federal laws have labeled as being “confidential”; or (2) could cause significant impact to the division or office in the form of financial loss or loss of credibility in the event of unauthorized disclosure; or (3) must be protected and accessible on a predetermined, need to know basis.
- Public – Assign the public level to applications with data that (1) state or federal laws have labeled as being “public”; or (2) is freely available and unrestricted.
- Internal Use Only – Assign the internal use only level to applications with data that can be appropriately labeled as such.

### 2. Determination of Risk (Refer to the DHHS Security Risk Management Policy)

If the established data classification is confidential or sensitive, then further classification must be made on the basis of risk. The DHHS Privacy and Security Office will develop a detailed process to determine these sub-categories; the following guidelines may be used:

- **Low** – Where an incident will likely have a limited adverse effect on agency operations (including mission, functions, image, or reputation), agency assets, or individuals. The event could be expected to cause a negative outcome or result in limited damage to operations or assets, requiring minor corrective actions or repairs.

- **Medium** – Where an incident will likely have a serious adverse effect on agency operations (including mission, functions, image, or reputation), agency assets, or individuals. The event could be expected to cause significant degradation in mission capability, place the agency at a significant disadvantage, or result in major damage to assets thereby requiring extensive corrective actions or repairs.
- **High** – Where an incident will likely have a severe or catastrophic adverse effect on agency operations (including mission, functions, image or reputation), agency assets, or individuals. The event could be expected to cause a loss of mission capability for a period that poses a threat to human life or results in a loss of major assets.

### 3. **Determination of Integrity Classification**

The DHHS Privacy and Security Office shall provide guidelines on how to determine the integrity classification of each business application used. Three (3) classifications of data integrity may be used:

- **Low** – Assign the low impact classification to applications with data that if destroyed or improperly altered could result in minor damage to division or office operations, minor financial loss or minor harm to individuals.
- **Moderate** – Assign the moderate impact classification to applications with data that if destroyed or improperly altered could result in significant damage to division or office operations, significant financial loss or significant harm to individuals. It would not involve loss of life or serious life threatening injuries however.
- **High** – Assign the high impact classification to applications with data that if destroyed or improperly altered could result in severe or catastrophic damage to division or office operations, major financial loss or major harm to individuals. The damage could involve loss of life or serious life threatening injuries.

### 4. **Application/System Classification of Availability (Refer to DHHS Business Continuity and Disaster Recovery Plan Policy)**

The availability classification is determined by the system owner, based upon the overall classification levels determined above. The recovery category determines how soon the application and the network should be available and on line after disaster or other malfunction. These classifications should be used in the Business Continuity and Disaster Recovery Plans and testing.

- Level One (overall security classification as high); 2 to 4 days
- Level Two (overall security classification as moderate or high); 5 to 9 days
- Level Three (overall security classification as moderate); 10 to 19 days
- Level Four (overall security classification as low); 20 or more days

### 5. **Data Classification Labeling and Access Controls**

The DHHS PSO shall provide guidelines on how to implement security controls to protect confidential or sensitive data. DHHS Divisions/Offices shall implement the appropriate safeguards.

Each DHHS Division/Office shall utilize more stringent security control requirements when the security level of an information system, facility, or network is designated as “high” level. In all instances, the minimum security requirements of a system should be appropriate for the highest security level designation of any data the DHHS Division/Office processes within that system, including data received from other agencies.

For each security level classification, controls must define protection of the following types of information processing activities:

- A. Copying;
- B. Storage;
- C. Transmission by mail, facsimile, Internet, intranet, and electronic mail;
- D. Transmission by spoken word, including mobile telephone phone, voicemail, and answering machines; and
- E. Destruction

Output from systems containing information classified as being sensitive or critical shall, as feasible, carry an appropriate classification label in the output. Items for consideration include printed reports, screen displays, recorded media (tapes, disks, CDs, cassettes), electronic messages, and file transfers.

Physical labels are generally appropriate; however, data in electronic form cannot be physically labeled, an electronic means of labeling may need to be implemented, as applicable.

The DHHS PSO shall develop and maintain enterprise-wide procedures to assist the DHHS Divisions/Offices on labeling data as well as provide guidelines for access control to that data including electronic marking and physical labeling.

## 6. Application/System Security Controls

All DHHS Applications/Systems shall implement the appropriate security controls to minimize risk in the production or operating environment. The type of controls necessary will be commensurate with the determination of data confidentiality or sensitivity, integrity and availability levels. The DHHS PSO shall define the controls necessary as part of the security certification methodology as defined in the DHHS Application Security Policy and Procedures.

## **Enforcement**

All DHHS disciplinary actions, up to dismissal for DHHS employees and/or termination procedures for contractors, shall be in compliance with relevant personnel and contract policies.

*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](#).