

DHHS POLICIES AND PROCEDURES

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

Purpose

To ensure that the appropriate information security controls are implemented for all of the Department of Health and Human Services (DHHS) applications.

Policy

To keep risk to an acceptable level, DHHS shall ensure that the proper security controls will be implemented for each application. These controls will vary in accordance with the sensitivity and criticality of each application. This policy addresses the following requirements: (1) application security standards and implementation guidelines; (2) the implementation of security controls during the system's lifecycle; and (3) security documentation.

Roles and Responsibilities

The DHHS Privacy and Security Office (PSO) shall develop enterprise-wide application security standards, procedures and guidelines.

The DHHS Divisions/Offices shall implement application security standards to have effective controls over systems they directly manage.

- If DIRM manages a DHHS Division/Office Information Technology Services (ITS) environment or application, DIRM shall be responsible for implementing the application security controls.
- If an outsourced contractor manages a DHHS Division/ITS environment or application, the division/office must ensure that the contractor implements the application security controls.

Implementation

Policy implementation shall comply with the DHHS management-approved standards and best practices. This policy follows [ITS Application Security Policy with Guidelines](#) and includes the following requirements:

1. Application Security Standards and Implementation Guidelines

The DHHS PSO shall develop and maintain application security standards and guidelines for implementing application security in the production environment. The development and maintenance of the standards and guidelines shall involve the appropriate responsible sections of the divisions/offices.

2. Security integrated within the Software Development Life Cycle (SDLC)

Security shall be an important part of the system life cycle process. Systems developed or acquired must have documented security specifications. In addition, all information technology services and systems must address the security implications of any changes made to a particular service or system.

A compilation of lifecycle documentation for the system shall be maintained and available for review in order to provide complete information on the system's security aspects. This documentation shall include:

- Application design and development
- Security controls
- Test plans and results
- Operations and maintenance documentation

The phase descriptions below may assist divisions/offices as they consider security requirements during the planning, design, implementation and operations of a new technology service. Information technology systems, services and programs require different levels of security.

A. Project Concept

Project concept development includes identifying a need and forming an initial approach. The following security tasks will be accomplished during this phase:

- Evaluate the security implications of new or revised information system(s) based upon the above security guidelines and the data classification requirements.
- Examine the functionality of the information system for the proposed system's functionality to determine which level of access is required by the system's user groups.
- Evaluate the system to determine if additional internal controls are required.
- Evaluate and document the *level of risk* to determine the severity of the adverse effect that an information system could cause as a result of non-evident failures or design flaws. This level of risk determination should also consider the data classification levels and criticality.

- Document the specific project security needs.

B. Project Requirements

Project requirements gathering involves collecting all the specifications that will determine the acceptance of the application/system. Security requirements shall be documented per federal and state requirements. Examples of user requirement statements for security aspects of the systems may include:

- Access Requirements
- General Requirements
- ITS Security Plan Requirements
- Change control Requirements
- Physical Security Requirements
- Security Banner Requirements
- Logon ID and Password Requirements
- Virus Protection Requirements
- Data Backup Requirements
- BC/DR Plan Requirements

Other Controls – The DHHS PSO may recommend other controls based on the data sensitivity and criticality of an application.

C. Project Design

Project design involves planning the various technical components of the application/system (e.g. architecture, database schema, interfaces, etc). During the design phase, security is evaluated in terms of the overall functional design specification. The information system design specification shall address the way in which the system security requirements will be implemented. This may include the following security elements as applicable, or reference other documentation for these elements: control logic, data structures, error and alarm messages, security measures, supporting software (e.g. operating system, drivers, other applications), communication links, interfaces, hardware links, special hardware needed, development standards and programming standards.

D. Implementation

Implementation involves the building, construction and/or coding of the software. This includes unit testing of individual software components. During the Implementation phase, a security code review shall be performed. Security test plans are constructed and a system contingency plan shall be drafted.

E. Testing and Installation

Before a system is placed into production, user functional requirements,

security requirements, and established controls shall be verified through systems testing. This testing shall determine that (1) user functional requirements are validated, (2) the system operates as designed; and (3) internal security controls work as intended. Testing shall be comprehensive, consistent, and repeatable with the comparison of expected results to actual test results and anomalies documented in the test summary report.

Test plans including test scripts and test results shall be documented and stored with system documentation for auditing purposes.

Post deployment testing shall be executed based upon approved changes to system configuration items, i.e., hardware, software, database configuration, etc.

F. Training

Training includes all activities necessary to prepare the workforce and public, to use, operate, support and maintain the system. This would normally be expected to occur before access to the system is permitted. Training will be documented and maintained by the system owner or designate.

G. Operations, Maintenance, and Retirement

Operations and maintenance involves day to day management of the system to ensure availability, integrity to meet user needs. This activity also includes changes deemed as system enhancements. Retirement involves decommissioning an application or system from the production environment. This phase includes the following security requirements:

1. Security Evaluation of Systems/Applications

DHHS PSO shall develop a method for evaluating the security of both new systems/applications as well as those already residing in production. This methodology shall consist of a verification component to ensure that all of the certification requirements were addressed and a validation component to ensure that the controls implemented work satisfactorily. Following this evaluation, a certification report on the status of each system shall be prepared.

2. Information System Security Certification and Recertification Process

The information system security certification process is the technical evaluation performed to determine the extent to which a particular computer system or network design and implementation meets a pre-specified set of security requirements. This evaluation may be performed either internally or by an external entity, as necessary. The

following paragraphs define the requirements for the security certification process:

- a. Determination of Data Confidentiality, Integrity and Availability in accordance with the DHHS Data Classification, Labeling and Access Control Policy.
- b. Preliminary risk assessment, risk protection strategies and risk protection profile in accordance with the DHHS Risk Management Policy and the ITS Risk Management Program.

The certified systems/applications of all DHHS Divisions/Offices must be recertified periodically (typically every three years, unless modifications are made that impact security) to ensure they still meet the security requirements.

3. Security Documentation

All security documentation (e.g., security plans, certification report, or external accreditation) shall be maintained, with copies sent to the Information Security Official of the responsible DHHS Division/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). 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](#).