

DHHS POLICIES AND PROCEDURES

Section VIII:	Privacy and Security
Title:	Security Manual
Chapter:	Security for Information Systems Contracts
Current Effective Date:	6/15/05
Revision History:	
Original Effective Date:	

Purpose

This policy defines the Department of Health and Human Services (DHHS) security requirements for those contracts that have been designated as Information Technology Services (ITS) or that have ITS components. All DHHS outsourced ITS contracts need to be written to ensure that federal and state regulations are met and that the security provided meets the level of security defined by DHHS Security Policies.

Policy

DHHS Divisions/Offices shall implement security requirements for DHHS third-party vendors of information systems and their components (hardware, software, people, data and system functions). The contract specifications shall meet state, federal and DHHS contracting policies ([DHHS Policy and Procedure Manuals, Section VII - Procurement and Contract Services](#)) and ITS privacy and security standards and procedures.

Roles and Responsibilities

The DHHS Privacy and Security Office (PSO) shall establish and maintain ITS contract security standards and provide guidelines for managing outsourced contracts. Contracts designated as ITS or with ITS components shall be reviewed by the Division of Information Resource Management (DIRM) as authorized by DHHS Directive II-12, based upon the established standards and criteria. The PSO, in collaboration with the DHHS Office of Procurement and Contract Office and the NC Attorney General's Office, shall develop and maintain contracting templates to address privacy and security requirements.

The DHHS Divisions/Offices shall be responsible for providing contract management oversight of the ITS contracts or this responsibility may be delegated to Division of Information Resources Management (DIRM) through written agreement. Divisions/Offices may add additional language to the contracts in order to meet division-specific funding requirements or implement division-specific procedures or reporting requirements.

The DHHS Division/Office Information Security Official shall be responsible for evaluating the security of all information systems for that division/office before they are placed into

production and making recommendations to improve security when deficiencies are observed.

Implementation

1. Establishing a Chain of Trust through DHHS Information Security Policies

Utilization of the approved contracting language and knowledge of and compliance with the DHHS Information Security Policies shall be implied upon signature of the contract.

2. Third Party Contract Security Requirements

ITS third party contract provisions shall address security concerns as appropriate to the scope and nature of the contract to meet legal and business requirements. Requirements may include:

- A. General policy on information security
- B. Asset protection, including:
 - 1. Procedures to protect organizational assets, including data and software;
 - 2. Procedures to determine whether any compromise of assets has occurred;
 - 3. Controls to ensure the return or destruction of information and assets at the end of, or at an agreed upon point during the contract;
 - 4. System data integrity and availability;
 - 5. Restrictions on copying and disclosing information.
- C. A description of each service to be made available;
- D. The target level of service and description or identification of unacceptable levels of service;
- E. Provisions for transfer of staff where appropriate;
- F. The respective liabilities of the parties to the agreements;
- G. Responsibilities with respect to legal matters, e.g., data protection legislation, especially taking into account different national legal systems if the contract involves cooperation with organizations in other countries;
- H. Intellectual property rights and copyright assignment and protection of any collaborative work;
- I. Access control agreements;
- J. The right to monitor and revoke user activity;
- K. The right to audit contractual responsibilities or to have those audits carried out by a third party. Any audits or reviews shall be conducted under the auspices of GS 143-6.1, OMB Circular A-133 and DHHS auditing practices.

- L. Provisions for annual or more frequent security audits or provide standards for adequate security and testing to insure that adequate security is being maintained. Consequences of a failure to pass the audit or review shall be included in the contract. Refer to the DHHS Information Systems Review and Audit policy for more specifications;
 - M. Establishment of an escalation process for problem resolution;
 - N. Responsibilities regarding hardware and software installation and maintenance;
 - O. A clear reporting structure and agreed reporting formats;
 - P. Clear and specified process for change management; any required physical protection controls and mechanisms to ensure those controls are followed;
 - Q. User and administrator training in methods, procedures and security;
 - R. Controls to ensure protection against malicious software. Vendors must supply a warranty that information system components contain no viruses, trojan horses, backdoors, malicious code or other programs that would allow anyone, including the vendor, unauthorized access to DHHS information systems;
 - S. Arrangements for reporting, notification and investigation of security incidents and security breaches;
 - T. DHHS participation with the third party in the selection, involvement and right of refusal with subcontractors;
 - U. Signed HIPAA Business Associate Agreement if applicable.
3. Security Requirements in Outsourcing Information Systems Development Contracts

Outsourcing information system development contract provisions may address the following security requirements in addition to the requirements of Section 2 above, as appropriate to meet legal and business requirements:

- A. The way in which legal requirements are to be met, e.g., data protection policy, standards and procedures;
 - B. The arrangements that will be in place to ensure that all parties involved in the outsourcing, including subcontractors, are aware of their security responsibilities;
 - C. The way in which the integrity, confidentiality and availability of DHHS business assets are to be maintained and tested;
 - D. The physical and logical controls that will be used to restrict and limit the access to DHHS sensitive business information to authorized users;
 - E. The way in which availability of services is to be maintained in the event of a disaster;
 - F. The levels of physical security to be provided for outsourced equipment;
 - G. The right of audit as referenced in Section 2.
4. Contract Termination

- A. Contract termination clauses must identify what is required to effect a successful transition, including vendor to vendor or vendor to state. A termination clause will identify all:
 - 1. Transition planning assistance,
 - 2. The specific written period of notice prior to the termination of the contract.
 - 3. Inventories of equipment, software and other assets that the service provider uses to provide the services,
 - 4. Copies of data, procedures, error logs, documentation and other information generated by the service provider as a part of providing services,
 - 5. Rights to hire people, buy/transfer the assets, license the software and assume the subcontracts used by the service provider to supply services.

- B. A contract that has been terminated and transferred to another vendor must address requirements for the new vendor to:
 - 1. Use facilities, software, equipment and subcontractors that DHHS owns or has a right to use;
 - 2. Implement a mirrored disaster recovery site for DHHS work specifically and a disaster recovery plan that DHHS could implement if the service provider's facility were destroyed, and
 - 3. Cooperate with DHHS in building internal capability or outside relationships to provide the same services that the outsourcer provides.

5. Contract Administration and Review

Contracts will be reviewed by each division/office/facility/school director or designee as follows:

- A. A representative sample of all existing contracts will be reviewed on an annual basis to determine compliance with this policy. This review will include:
 - 1. Defining, developing and documenting contract audit procedures for applicable regulations, i.e., HIPAA, DHHS policies;
 - 2. Selecting appropriate reviewers;
 - 3. Scheduling periodic contract reviews using the defined procedures, and
 - 4. Reporting review findings and making these findings available for review including:
 - a. Review scope;

- b. Number of transactions or contracts sampled, number of identified deficiencies, potential suggestions for corrective actions, and time frames for corrections, and
 - c. Implementing a corrective action system (see DHHS Risk Management policy).
- B. Review findings shall be reported to designated staff in accordance with division/office policy or procedure. This may include program manager/supervisor, contract administrator or division/office security official.

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](#).