

DHHS POLICIES AND PROCEDURES

Section VIII:	Privacy and Security
Title:	Security Manual
Chapter:	User Authorization, Identification and Authentication Policy
Current Effective Date:	6/15/05
Revision History:	
Original Effective Date:	

Purpose

To define the security requirements for setting up user accounts, enabling user access and ensuring the user is properly authenticated at the Department of Health and Human Services (DHHS) Divisions/Offices. To mitigate the risk of unauthorized access of information, establish user accountability and rules for access.

Policy

DHHS shall require that systems are protected from unauthorized access by establishing requirements for the authorization and management of user accounts, providing user authentication (via logon identifiers and passwords), and implementing access controls on DHHS information resources.

As applicable, the [DHHS Privacy Manual](#), "Use and Disclosure Policies" and the enterprise North Carolina Identity (NCID) standards and procedures will serve as the base requirements. Any additional requirements developed will be in compliance with federal and state regulations and standards.

Roles and Responsibilities

The DHHS Privacy and Security Office (PSO) shall provide user identification standards for the DHHS Divisions/Offices. The PSO shall also provide enterprise-wide procedures and guidelines for managing user accounts and implementing access controls.

Workforce roles associated with this policy are:

- DHHS System Owners - System owners for each information system shall be responsible for ensuring that authorization and account management processes exist for their specific division/office and that the appropriate people have been assigned the responsibility of creating and maintaining the authorization records. The design and development of the authorization and account management processes shall comply with DHHS security standards.

DHHS Division/Office System Owners may monitor and/or review the privacy and security policies and operations of an agency, contractor/vendor or individuals as a condition for granting access or as a condition for continued access to information resources.

- Managers/Supervisors - DHHS managers/supervisors have the responsibility of requesting access to information systems and approving user access privileges based upon their assigned duties and notifying the system administrator of changes in access status.
- System Administrators - System administrators have the responsibility of periodically reviewing user access privileges and notifying management of any access concerns. This responsibility may lie with the Division of Information Resource Management (DIRM), an outsourced contractor or within the DHHS Division/Office but shall be in compliance with standards established by the DHHS PSO.

Implementation

Policy implementation shall be based upon the use of management-approved security standards, procedures and industry best practices. Newly developed applications shall follow the NCID standards as appropriate. Any existing applications will be assessed to determine feasibility of migration to NCID standards as enhancements or upgrades are planned. Other systems and applications shall follow the requirements listed below. Requirements associated with the source of funding shall be incorporated into the division/office procedures.

1. IS Authorization and Account Management

The following paragraphs specify the requirements for information system authorization and account management:

A. Access Authorization and Account Management Process

Each division/office shall implement a process and document procedures for granting users access to information resources. These procedures must be in compliance with established Information Technology Services (ITS), DHHS standards and specify the requirements for initial access, modification of access, or termination of access as noted in this policy.

An automated process, NCID requires an enterprise wide registration form and procedures that include self-registration followed by approval of the subscription process. The subscription process may be implemented at the department, division or application level. Additional requirements may be obtained during the subscription process.

If access is a condition of funding, the division/office shall maintain the documentation of the funding requirement. The documentation should provide the purpose of access and use of data. The conditions of acceptable use and disclosure should be in compliance with the DHHS Privacy Manual. If the conditions are not covered within the existing DHHS Use and Disclosure policies, additional documentation will be required. The *Application and Authorization for Access to State Automated System Form* may be used as a template.

B. Initial User Access Evaluation and Approval

Prior to being granted access to DHHS computer resources, the needs of every employee, contractor, vendor, guest, or volunteer shall be given ample consideration and authorization granted to allow access to DHHS resources. This shall be a formal process, whereby authorization is approved and a record of what resources the individual is allowed to access is kept on file in accordance with NCID procedures or as listed below.

The *Application and Authorization for Access to State Automated Systems Form* may serve as a template for granting or modifying access to automated systems owned by DHHS.

Authorization should include the following:

- Access is limited to the information resources described on the request;
- The data will be used only by the authorized individual;
- The data will be used only for the purpose stated on the request;
- A new request will be submitted if there are any changes to the stated conditions of access;
- The authorization request, if in hardcopy format must be signed by the applicant and approved by the supervisor or manager assigned, and
- The authorization request, if electronic, must identify the supervisor or manager making the request.

Access Authorization will need to be established or reviewed under the following conditions:

- A new employee is hired;
- The worker transfers to another area resulting in job function changes;
- Employment for the worker terminates;
- The worker requires additional functions or access to fulfill a specific duty, or
- The worker no longer requires access.

DHHS Divisions/Offices reserve the right to revoke access if the conditions of access are not met.

The documentation of the approval/denial shall be maintained in accordance with Record Retention Laws, NCGS 132-3, GS 121-5 and General Schedule for State Agency Records. HIPAA regulation 45 CFR 164.316 (b)(2)(i) requires that security related documentation be retained for six (6) years from the date of its creation or the date when it last was in effect, whichever is later. For additional information see the DHHS Records Management policy.

C. Access Modification

Requests for modifying user accounts (i.e., to grant or disallow additional permissions) shall be accomplished by submitting a new request. The request, if in hardcopy format, must be signed by the applicant, supervisor or manager assigned. Electronic requests must identify the supervisor or manager making the request.

D. Emergency Access

Requests for temporary emergency access must also be documented.

E. Access Termination

When a user is transferred or terminated, the user's access to system data must be terminated to minimize risk while preserving the User's records and data stored locally or in network directories. It is the responsibility of the direct supervisor or manager to contact the system owner and the system administrator immediately when the user is transferred or terminated.

F. Audits of User Access Rights

The system owner of each information system shall ensure that all user accounts are reviewed and access rights evaluated at least once per quarter. Discrepancies must be investigated and corrected. Audit documentation will be maintained as specified by the DHHS Security Policy for Records Management.

2. User Identification and Authentication

The following paragraphs specify the requirements for user identification and authentication to DHHS information processing systems. These requirements must meet the [ITS Identification and Authentication Using IDs and Passwords Policy](#) and Standards.

A. User Authentication

User Identification and Authentication is an access control methodology. At a minimum, DHHS uses a two-factor (an assigned user ID and user specified password) approach to determine a user's identity, verify that it is correct, and establish accountability. All DHHS users shall be responsible for the actions performed through their account. User ID's can be:

- Randomly generated;
- A defined prefix and random suffix, or
- A defined prefix or suffix with a choice of other characters.

B. User ID and Password Protection

A computer logon ID or account is a combination of letters and numbers assigned to a particular user. Logon ID's are unique and shall not be replicated. A user-selected password is required to authenticate the user and grant access to the DHHS resources.

The DHHS PSO shall publish enterprise-wide procedures on user authorization, logon identification, password selection, password management and user authentication.

3. Logical Access Controls

The following paragraphs specify the Logical Access Control Security Requirements.

A. Access Rights

All access rights or privileges granted shall be documented and kept on file for review/audit purposes.

B. Access Controls

Access controls shall be implemented to protect information resources within the DHHS ITS environment. Only management-approved access control software (e.g., RACF, ITS or DIRM standards) may be used to restrict access in the production environment. Access to security software shall be limited to security administrators and officials and authorized personnel.

Logical access controls may be implemented on applications, databases and database management systems (DBMS). These controls will have the effect of limiting access to data based upon the principle of least privilege.

C. Login Attempts

The number of consecutive attempts to enter an incorrect password shall be limited to prevent password guessing attacks. After three (3) unsuccessful attempts to enter a password, the involved user-ID shall be either: (a) suspended until reset by a system administrator, (b) temporarily disabled or (c) if dial-up or other external network connections are involved - disconnected.

D. Multiple On-line Sessions

To ensure individual accountability, users will not be allowed to conduct multiple simultaneous on-line sessions without management approval.

E. Restricted Access after “No Activity” Period

If there has been no activity on a computer terminal, workstation, or microcomputer (PC) for a period of time (typically 10 to 15 minutes) the system must automatically either blank the screen or use a screen saver image, and restrict access. Re-establishment of access may occur after the user has logged back on to the system

F. Emergency and Temporary Access

Emergency access is immediate and is typically granted to correct a problem that may result in further damage if not corrected. Emergency and temporary access authorization shall be controlled. Temporary access is access granted for time limited basis for a specific purpose. Emergency and temporary access authorizations shall be: (a) documented, approved and maintained on file by the appropriate managers; (b) communicated to the DHHS information security officer, associated with the DHHS Division/Office and (c) automatically terminated after a predetermined period.

G. DHHS Authentication Methodologies

The DHHS PSO shall develop authentication standards and implementation guidelines. Technologies used may include tokens, smartcards, digital certificates or other access control mechanisms selected on the basis of acceptable risk.

H. Third-Party Network Connectivity

All third-party (e.g., business associates, vendors, etc) network connection requests shall be evaluated and approved by management. The connection

request will typically contain the following items:

- List of DHHS resource(s) that must be accessed and for what purpose;
- Sensitivity or criticality of the information resource(s) involved;
- Hours of access, start date, and end date for connection requested;
- Estimated number of users;
- Detailed description of use;
- Communication protocol(s) hardware, software, and any special requirements;
- Request for information resource access forms;
- Connectivity description;
- Connectivity risk assessment;
- Completed business associate access request form;
- Authorized third-party network service(s) to be used for the connection;
- Escalation procedures with contact information, and
- Performance requirements.

Third party access shall be limited to those services and/or devices that are needed to perform the required business function.

I. Remote Access

All remote access implementations shall conform to the ITS Remote Access Security Standard and the DHHS Acceptable Use Policy. The DHHS PSO shall develop enterprise-wide procedures to support remote access implementations at the DHHS Divisions/Offices.

DHHS personnel working off-site shall only use management-approved computer software, hardware, and virus protection software when working on DHHS business. Remote access to the DHHS network and resources shall be permitted upon authentication of authorized users.

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*](#).

North Carolina Department of Health and Human Services

**Application and Authorization for Access to DHHS Automated Systems
Users, Third-Party, and Vendor Access Form**

Part I: Applicant

The purpose of this form is to establish, modify, or terminate authorization for access to automated systems owned by the Department of Health and Human Services (DHHS). The applicant agrees to ensure that only the automated systems described here are used, that they are used only by the individual listed here, and that they are used only for the purposes stated here. Any changes to these stated conditions must be requested by submitting a separate amended copy of this form to the DHHS Security Official. Any other individual requesting access must complete a separate application for access. The Department of Health and Human Services reserves the right to revoke access if these conditions are not met.

Part I: This part must be completed by the organization and applicant requesting access establishment, modification, or termination.

Complete Part I for each applicant.

Applicant Information
Applicant Name:
Title:
Department:
Phone:
Status: <input type="checkbox"/> Full Time <input type="checkbox"/> Contractor <input type="checkbox"/> Part Time <input type="checkbox"/> Temporary
Location:
Manager's Name:
Manager's Phone:

Network Access				
Network Name	Establish	Modify	Terminate	Comments (include group permissions if applicable)
Novell Network	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Windows Network	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
AS400	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Oracle	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
RACF	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Other	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

System Access				
System Name	Establish	Modify	Terminate	Comments (include group permissions if applicable)
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

DHHS Division which owns the system: _____

Division contact person: _____

Title: _____ Telephone: _____

Are you currently accessing any other North Carolina automated system(s)? ___ yes ___ no

If yes, what is/are your user id(s)? _____

For Applicant's Signature Only

By signing this document, I signify that I have read, understand, and agree to abide by the DHHS computer use policy.

Applicant's Signature: _____ Date: _____

For Supervisor/Manager Use Only

Responsible Manager shall complete and sign this section:

Authorized Signature: _____ Date: _____

Print Name and Title: _____

Phone Number: _____

North Carolina Department of Health and Human Services
Application and Authorization for Access to DHHS Automated Systems
Users, Third-Party, and Vendor Access Form

Part II: Division

Completion of Part II constitutes authorization by the division for access and use of the systems described in Part I by the individual and organization described in Part I and indicates that the division agrees to arrange all matters involved in providing access, technical support, and training for the use of the system.

Part II : This part must be completed by the division and section which owns the system(s) described in Part I.

Name of Division: _____

Name of Person Authorizing Access: _____

Title: _____

Section: _____ **Telephone:** _____

Signature: _____ **Date:** _____

Name of Division System Contact: _____

Title: _____

Section: _____ **Telephone:** _____

Signature: _____ **Date:** _____

Return Completed Form To:

DHHS Division/Office Security Official and System Administrator

Part III: DIRM Use Only

Date: _____

Applicant User ID assigned: _____ **Billing Code assigned:** _____
