

Number: AS-PT-06-001

Issue Date: 01/20/2006

Authorized Signature _____

Topic: Agency-wide Policy

Transmitting (check the box that best applies):

- New Policy
 Policy Change
 Policy Clarification
 Executive Letter
 Administrative Rule
 Manual Update
 Other: _____

Applies to (check all that apply):

- All DHS employees
 County Mental Health Directors
 Area Agencies on Aging
 Health Services
 Children, Adults and Families
 Seniors and People with Disabilities
 County DD Program Managers
 Other (please specify):

Policy/Rule Title:	DHS Information Access Control Security Policy		
Policy/Rule Number(s):	DHS-090-003	Release No:	3.0
Effective Date:		Expiration:	
Reference:	Forms: DHS 780; DHS 781; DHS 782; DHS 783; DHS 784 and DHS 785 Procedures: DHS-090-003-01 and DHS-090-003-02		
Web Address:	http://www.dhs.state.or.us/policy/admin/security/090_003.htm		

Discussion/Interpretation:

This Agency-wide policy transmittal is being sent to all DHS staff. DHS Computer Systems are an integral part of DHS daily activities. Currently standards do not exist that either track if the user has the minimum necessary access to computer systems, or identify who gives permission for computer access to the user.

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule and the Secretary of State Audits identify the need for a tracking mechanism for both internal and external user access. Only authorized users shall have access to specific computer systems.

The DHS-090-003 Policy is being amended to ensure secure information access. These six new forms are designed to support DHS managers and contract

administrators in their efforts to identify and authorize specific computer access for users:

- The “Individual User Profile/Stand-Alone” form (IUP-DHS 0780)
- The “Individual User Profile/Cluster-Specific” forms (HS-DHS 0781; OMAP-DHS 0782; CAF-DHS 0783; and SPD-DHS 0784)
- The “DHS Contract Systems Information Exchange Assessment” form (DHS 0785)

Two new procedures will instruct DHS managers and contract administrators on how to complete the six new forms:

- The DHS-090-003-01 “Individual User Profile-Internal Access (DHS Employees/Authorized Partners)”
- The DHS-090-003-02 “Individual User Profile-External Access (Contracting business Entity)”

Implementation Instructions for Internal Users:

Managers begin using the IUP forms for all DHS internal users, and are to complete the process of identifying existing users and their authorized level of access over the course of one year (could be linked to new hires, annual staff performance evaluations, anniversary dates, position description changes, etc., but are not limited to these events).

- Managers keep the completed IUP forms in a secure location (e.g., the personnel employee file, etc.) readily available upon request.
- When the access privileges change, managers review the IUP (e.g., promotion, demotion, rotation, developmental, extended leave, termination, etc.) or at a minimum annually.
- Managers complete the annual “Safeguards Assessment Tool” (DHS 3000). *This tool will have a section where managers will be able to indicate their level of compliance with the required review of Access Control. This will allow the ISO to track compliance.*

Transition Process for Internal Users:

The ISO will collaborate with the various clusters (HS, OMAP, CAF, SPD, etc.) as required. This interaction will address questions and concerns as they surface during this yearlong rollout period for our internal partners.

Implementation Instructions for External Users:

Contract administrator begins assisting Contracting Business Entity (CBE) through the process of identifying external users and their authorized access over the course of one year (could be linked to new and amended contracts etc., but are not limited to these events).

- When a contract requires access, or exchange of access to or from DHS computer systems, contract administrator will assist the CBE with completing the “DHS Contract Systems Information Exchange Assessment” (DHS 0785) form.

- When a contract requires individuals to access applications, in order to provide the contracted services, contract administrator informs CBE that they are required to use the IUP (DHS 0780 – 0784) form (or a comparable CBE supplied form)
- When a contract requires the completion of an IUP form, contract administrator/Local DHS Contact informs CBE that they are required to keep the IUP form (or the comparable form) in a secure location, readily available upon request.
- When a contract grants access to DHS computer systems, the contract administrator/Local DHS Contact informs CBE that they are required to establish an access control review process (annually at a minimum).
- When a contract allows DHS access to contractor information, and the contractor has their own security requirements, the contract administrator/Local DHS Contact informs CBE that the Information Security Office (ISO) will perform an information security risk assessment to determine DHS' ability to meet those requirements.
- Contract administrator shall contact their program's contract writer for contract-related guidance when deemed necessary. *Updated contract language now supports information access control security requirements.*

Transition Process for External Users:

The ISO will collaborate with the various clusters (HS, OMAP, CAF, SPD, etc.) as required. This interaction will address questions and concerns as they surface during this yearlong rollout period for our external partners.

Training/Communication Plan:

This policy amendment transmittal provides formal announcement of the policy change. A training plan will be implemented, using a variety of methods (e.g., Web Based, NetLink, classroom, etc.).

Security and Privacy information can be found in the "[Privacy/Security Update](#)" newsletter. Additional resources may include departmental monthly newsletter and tools provided to managers for staff training.

Local/Branch Action Required:

Effective immediately after this transmittal, all CAF staff are expected to transition to the (CAF-DHS 0783) IUP form. CAF Child Welfare/Self Sufficiency staff will cease to use the temporary Individual User Profile (DHS 0785T). However, managers will retain the DHS 0785T and at time of review for staff access, will complete a CF-DHS 0783 IUP for the affected staff.

Central Office Action Required: The Information Security Office (ISO) will respond to any questions or concerns; review the policy and procedures annually and update as necessary; and inform staff of resulting impact as a result of a change.

The ISO will assume responsibility for facilitating the "Information Access Control Contract Project (IACCP)" and the "Information Access Control Manager Project

(IACMP)". The ISO anticipates that the projects may require a time commitment of a full year and hereby accepts this obligation.

Field/Stakeholder review: Yes No

If yes, reviewed by: Information Security Office, Policy and Procedures Development Team and Department-wide Support Services (DWSS) Required Reviewers.

Filing Instructions: No paper copies are distributed for filing. DHS Agency-wide policies are located on the DHS web site at <http://www.dhs.state.or.us/policy/admin/>

If you have any questions about this policy, contact:

Contact(s):	Kyle Miller		
Phone:	503-945-6812	Fax:	503-947-5396
E-mail:	dhsinfo.security@state.or.us		