SHARED SERVICES
OFFICE OF INFORMATION SERVICES
Information Security and Privacy Office

Operational Policy

Policy title:	Access Control Policy		
Policy number:	DHS|OHA 090-003		
Original date:	01/29/2006	**Last update:**	06/04/2018
Approved:	Don Erickson, DHS Chief Administrative Officer, Kris Kautz, OHA Deputy Director		

Purpose

Department of Human Services (DHS) and the Oregon Health Authority (OHA) is committed to controlling, securing, and protecting information created and maintained by the agencies by enacting requirements for accessing DHS|OHA information assets and systems.

Description

This policy establishes the requirements for controlling, securing, and protecting access to DHS|OHA information assets.

Applicability

This policy applies to all DHS|OHA staff including employees, volunteers, trainees, interns, contractors, and partners.

As keepers of the public trust, all agency employees have a responsibility to comply with state and agency policies, administrative rule, and state and federal law. The agency takes this responsibility seriously and failure to fulfill this responsibility is not treated lightly. Employees who fail to comply with state or agency policy, administrative rule, or state and federal law may face progressive discipline, up to and including dismissal from state service. Contractors and partners may face termination of the working relationship as well as federal sanctions.

Policy

1. DHS|OHA shall establish policies, processes, and guidelines ensuring DHS|OHA control access to information assets and systems.
2. DHS|OHA shall protect information assets and systems through administrative, physical, and technical controls and safeguards, including identification verification, password protection, data encryption, secured facilities, and agency policies to prevent unauthorized access, use, modification, destruction, or disclosure of information and data unavailability.
3. DHS|OHA shall maintain an inventory of information systems, and update that inventory at least annually.
4. DHS|OHA shall clearly label and store data, in accordance with federal and state statute and rule.

5. Authorized users shall receive access to DHS|OHA information assets, systems, and data in accordance with approved policies and processes, and approved, role-based user roles.
   a. An individual's manager shall approve access for internal users of DHS|OHA information systems, including remote access based on job duties and the user's role.
   b. Program staff, in collaboration with the information system owner and the Information Security and Privacy Office (ISPO), shall determine external user access to DHS|OHA information systems.
6. Members of the DHS|OHA workforce shall adhere to established processes for gaining, granting, modifying, or revoking access to agency information and information systems, and for providing access to external users.
7. Any user account shall not be used as a service account.
8. Access control shall include the requirements for:
   a. Role-based access controls (ensuring that individuals have access necessary to perform their job functions).
   b. Account management (creating, changing, and removing user accounts, providing access to network resources, network and information system suspension, and the use of warning banners to safeguard system use).
   c. Account authentication (user, system, and password controls for individuals accessing information systems, with additional controls for protected information).
   d. Separation of duties (required separation of job roles for individuals approving system access, providing system access, and auditing access levels).
   e. Management of passwords (system requirements for creating and changing passwords, including the frequency of password changes based on data access, the required complexity of passwords based on program requirements, and guidelines for safeguarding passwords).
   f. Network access suspension (monitoring and lock-out for excessive log-in attempts, automatic revocation of access due to non-use, and suspension during extended leave periods).
   g. Session control (establishing and ensuring performance of system limits to the ability to sign in to individual systems from multiple locations at the same time and limiting the amount of time a log-in session remains active before self-locking or self-terminating).
   h. Remote access (setting standards and processes for individuals or entities to gain access to information systems from a non-agency location).
   i. Wireless access (setting standards and processes for the approval of individual wireless access to DHS|OHA systems).
   j. Mobile devices (approval and security standards and processes ensuring agency issued or approved personal devices are secure when accessing DHS|OHA systems).
   k. External information systems (setting standards and processes for risk evaluation and security management planning, allowing DHS|OHA systems to access external systems).
   l. External web administration (approval process for posting agency materials to the DHS|OHA public website).
9. DHS|OHA access control processes shall include the requirements for establishing, documenting, reviewing, modifying, and terminating an individual's right of access to DHS|OHA systems.
10. Before access is provided to DHS|OHA systems, a background check shall be completed in accordance with Human Resources policies.
11. Information system owners shall review who has access to their system at least annually.

12. All members of the DHS|OHA workforce shall follow access control processes throughout the life cycle of electronic information assets, including using the secure email system for the electronic transmission of protected information, and the transmission of data through electronic means.
13. The Office of Contracts and Procurement shall include security language in all contracts where the contract administrator identifies a need for the contractor's or subcontractor's access to DHS|OHA information systems.
14. Contract administrators shall review contractor access rights:
    a. When a contract is negotiated, initiated, amended, or renewed.
    b. In response to security incidents.
15. The Chief Information Risk Officer (CIRO) may require specific access controls be applied to any contract.
16. DHS|OHA shall follow all applicable agency, state and federal law and requirements, and Oregon statewide policies.

References

45 CFR 160 & 164

OAR 125-055-0100 to 125-055-0130

OAR 943-014-0300 to 943-014-0465

Centers for Medicare & Medicaid Services: Minimum Acceptable Risk Standards for Exchanges

Criminal Justice Information Systems Security Standards (CJIS)

Federal Information Processing Standards (FIPS) Publication (Pub) 199

Federal Information Processing Standards (FIPS) Publication (Pub) 200

IRS Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev. 4

Social Security Administration Information Exchange Security Requirements and Procedures

DHS|OHA-090-003-01 Privileged Access and Management Process

DHS|OHA-090-003-02 Privileged Access and Management Process Map

DHS|OHA-090-003-03 Information System Non-Local Maintenance Guidelines

DHS|OHA-090-003-04 Password Guidelines

DHS|OHA-090-003-05 User Access Process Employees

DHS|OHA-090-003-06 User Access Process Employee Map

Forms referenced

MSC 0785 Third Party Information System Access Request

MSC 0786 DHS|OHA Individual Access Request Form

Related policies

DAS 107-004-050 Information Asset Classification Policy

DAS 107-004-052 Information Security

DHS-020-001 Public Contracting Authority and Overview for Supplies and Services Contracts

DHS-060-010 Background Checks

DHS-060-007 Employee Separation

Contact
Information Security and Privacy Office
Security 503-945-6812
Dhsinfo.security@state.or.us

This policy shall be reviewed at least once every year to ensure relevancy.

Policy history

Version 1 DHS-090-003 established 12/10/2002
Replaced by joint policy
Version 1 DHS|OHA-090-003 established 03/11/2015
Version 2 DHS|OHA-090-003 reviewed annually 03/04/16
Version 3 DHS|OHA-090-003 revised 06/04/2018

Keywords

Access, access management, access control, access agreements, assets, contract, diagnostic, hardware, local maintenance, maintenance, mobile devices, NIST, non-local maintenance, procurement, remote access, repair, role-based, user access, wireless

---

This document can be provided upon request in an alternate format for individuals with disabilities or in a language other than English for people with limited English skills. To request this document in another format or language, contact the Publications and Design Section at 503-378-3486, 7-1-1 for TTY, or email dhs-oha.publicationrequest@state.or.us.