Operational Policy

Policy title:	Access Control Policy		
Policy number:	ODHS|OHA 090-003		
Original date:	01/29/2006	**Last update:**	08/02/2021
Approved:	Kris Kautz, OHA Deputy Director Don Erickson, ODHS Deputy CAO		

Purpose

The Oregon Department of Human Services (ODHS) and the Oregon Health Authority (OHA) are committed to controlling, securing, and protecting information created and maintained by the agencies by enacting requirements for accessing ODHS|OHA information assets and systems. The purpose of this policy is to ensure users have the appropriate access levels specifically authorized to them to access information on information systems and applications, and that individuals understand the responsibility their access level provides them.

Description

This policy establishes the requirements to protect ODHS|OHA information assets and systems against improper or unauthorized access that could result in the compromise of confidentiality, integrity, or availability of ODHS|OHA information, information technology (IT) assets, or technology-enabled capabilities.

Applicability

This policy applies to all ODHS|OHA staff including employees, volunteers, trainees, interns, as well as 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. ODHS|OHA shall protect information assets and systems through administrative, physical, and technical controls and safeguards.
   a. Administrative controls include policies, processes, and guidelines ensuring ODHS|OHA controls access to information assets and systems.

   b. Physical controls limit physical access to electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.
   c. Technical controls specify the technology utilized to protect access to information assets and systems.
2. ODHS|OHA shall clearly label and store data, in accordance with federal and state statute and rule.
3. ODHS|OHA system owners shall approve access to information systems to ensure that data use meets business needs and matches their approved user roles.
   a. Approved authority shall approve access for internal users of ODHS|OHA information systems, including remote access based on job duties and the user's role.
   b. Third party entities shall be approved for access per the Third Party Entity Approval for System Access Process (ODHS|OHA 090-003-08), and shall also be approved by an ODHS|OHA sponsoring manager.
4. Authorized users shall respect the confidentiality of other users' information and shall not attempt to share or obtain other authorized users' access log in credentials.
5. Any user account shall not be used as a service account or a shared login. A service account is a type of account that an application or server uses to interact with the operating system.
6. Access control shall meet the Statewide Information and Cyber Security Standards.
7. Only agency-owned and managed devices shall have direct access to secure production wireless networks in ODHS|OHA locations.
8. Federal tax information (FTI) shall only be accessed or used by ODHS|OHA staff in accordance with the Internal Revenue Services (IRS) Publication 1075 and OAR 407-007-0020(1).
9. Criminal Justice Information (CJI) shall only be accessed or used by ODHS|OHA staff in accordance with the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy and OAR 407-007-0020(1).
10. CJI shall only be accessed or used by ODHS|OHA contractors and partners in accordance with FBI CJIS Security Policy, CJIS Security and Management Control Outsourcing Standard for Non-Channelers, and OAR 407-007-0020(1).
11. Social Security Administration (SSA) data shall only be accessed or used by ODHS|OHA staff in accordance with the SSA's Information System Security Guidelines.
12. ODHS|OHA access control processes shall include the requirements for establishing, documenting, approving, modifying, and terminating an individual's right of access to ODHS|OHA systems.
13. Before access is provided to ODHS|OHA systems and data, a background check shall be completed in accordance with Human Resources policies.
14. Information system owners shall review who has access to their system at least annually.
15. Managers shall review their employees' access annually for least privilege and remove access as appropriate. Least privilege means allowing only authorized accesses for users, or processes acting on behalf of users, that are necessary to accomplish assigned tasks in accordance with ODHS and OHA's mission and business functions.
16. 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 ODHS|OHA information systems.
17. Contract administrators shall review contractor access rights:
   a. When a contract is negotiated, initiated, amended, or renewed.

b. In response to security incidents.

18. The Chief Information Risk Officer (CIRO) shall require specific access controls be applied to any contract.
19. Access requests shall be maintained in the service desk ticketing system for auditing purposes.

References

45 CFR 160 General Administrative Requirements
45 CFR 164 Security and Privacy
OAR 125-055-0100 to 125-055-0130 HIPAA Privacy and Security Rule Implementation; HITECH Act Implementation
OAR 943-014-0300 to 943-014-0465 Privacy and Confidentiality
OAR 407-007-0000 to 407-007-0100 Criminal Records Checks for the Department of Human Services
OAR 407-007-0400 to OAR 407-007-0460 Abuse Checks for Department Employees and Volunteers
OAR 943-007-0001 Criminal History Checks
OAR 943-007-0501 Background Checks for the Oregon Health Authority
OAR 943-014-0300 to 943-014-0465 Privacy and Confidentiality
Center for Internet Security Top Twenty Critical Security Controls
Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy
FBI CJIS Security and Management Control Outsourcing Standards for Non-Channelers
IRS Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies
MARS-E Document Suite, Version 2.0, Volume III: Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges
National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev. 5
NIST Risk Management Framework in support of the Federal Information Security Management Act (FISMA)
ODHS|OHA 090-003-01 Privileged Access and Management Process
ODHS|OHA 090-003-02 Privileged Access and Management Process Map
ODHS|OHA 090-003-04 Managing Password Process
ODHS|OHA 090-003-05 User Access Process Employees
ODHS|OHA 090-003-06 User Access Process Employee Map
ODHS|OHA 090-003-08 Third Party Entity Approval for System Access Process
ODHS|OHA 090-003-09 Third party Entity Approval for System Access Process Map
Privacy Act, 5 U.S.C. 552a, Section 1106 of the Social Security Act
Social Security Administration Information Exchange Security Requirements and Procedures
Statewide Information and Cyber Security Standards 2019

Related policies

DAS 107-004-050 Information Asset Classification Policy
DAS 107-004-052 Cyber and Information Security
DAS 107-011-170 Building Security Access Controls Policy
ODHS|OHA 010-018 Records Retention and Management Policy

ODHS 020-001 Public Contracting Authority and Overview for Supplies and Services Contracts
ODHS 060-010 Background Checks
ODHS 060-007 Employee Separation

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

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

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
Version 4 ODHS|OHA 090-003 revised 08/02/2021

Keywords
Access, access control, administrative controls, annual review, assets, criminal justice information, CJI, federal tax information, FTI, Internal Revenue Service, IRS, physical controls, role-based, technical controls, user access wireless

---