

Process steps

Title:	ODHSOHA 090-003-05 User Access Process
Related to:	ODHSOHA 090-003 Access Control Policy
Effective date:	12/04/2023

Purpose

This document illustrates the step-by-step process by which the Oregon Department of Human Services (ODHS) and the Oregon Health Authority (OHA) provide unique user identification and add, modify, move, or delete an individual employee's user profile to create, alter, or remove access to agency information, networks, and email systems.

Applicability

This process applies to all ODHS and 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.

Process Steps

1. Individuals placed in the state Human Resources Management Systems (HRMS), receive baseline access as approved by ODHS and OHA management and are automatically granted upon the individual being validated as an active ODHSOHA individual in HRMS.
 - a. Baseline access includes identity in the approved authorization system, access into agency computers and network, email, calendar and the ODHSOHA Intranet.
 - b. The remainder of these steps must be followed for all other system access. No other access is granted until step one is complete.
2. For individuals not placed in HRMS, the approving or sponsoring ODHS or OHA manager or designee of the individual requesting access confirms that the individual's background check has been completed.
3. The approving or sponsoring ODHS or OHA manager or designee:

- a. Completes an Individual Access Request (IAR 786) through Service Desk Online to obtain needed access.
 - A. If onboarding, ensure the “effective date” is the first day of employment and go to steps 3b and 3c.
 - B. If offboarding, ensure the “effective date” is the last day of employment and skip steps 3b. and 3c.
 - b. Completes any necessary program specific forms for access to other systems in preparation for submission. Some applications may require additional unique user identifications and additional information.
 - c. Attaches the program specific forms to the IAR 786 in Service Desk Online.
4. Requests are automatically recorded in the OIS approved ticketing system.
5. OIS:
- a. Confirms with HRMS/Human Resources that the individual for whom access is requested is authorized to access ODHSOHA systems. This is not required for offboarding or for contractors and partners.
 - b. Forwards the IAR 786 extract and the program specific forms to the appropriate assisting work group to complete the request. The appropriate assisting work group documents the work performed in the OIS approved ticketing system.
 - c. Coordinates and provides the access as requested and approved. When the work is completed, automated notification is sent to user and requestor as appropriate.

References

[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](#)

[MARS-E Document Suite, Version 2.0, Volume III: Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges](#)

[Criminal Justice Information Systems Security Standards \(CJIS\)](#)

[Federal Information Processing Standards \(FIPS\) Publication \(Pub\) 199 Standards for Security Categorization of Federal Information and Information Systems](#)

[Federal Information Processing Standards \(FIPS\) Publication \(Pub\) 200 Minimum Security Requirements for Federal Information and Information Systems](#)

[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. 5 Security and Privacy Controls for Information Systems and Organizations](#)

[Social Security Administration Information Exchange Security Requirements and Procedures](#)

[ODHSOHA 090-003-06 User Access Process Map](#)

[ODHSOHA 090-003-08 Third Party Entity Approval for System Access Process](#)

[ODHSOHA 090-003-09 Third Party Entity Approval for System Access Process Map](#)

[ODHSOHA 090-003-016 Baseline Access Process in Information Technology](#)

[ODHSOHA 090-003-017 Baseline Access Process in Information Technology Process Map](#)

[Center for Internet Security Critical Security Controls](#)

[Statewide Information and Cyber Security Standards](#)

Forms referenced

[IAR 786 Individual Access Request](#)

Related policies

[DAS 107-004-052 Cyber and Information Security](#)

[ODHSOHA 060-010 Background Checks](#)

[ODHSOHA 060-007 Employee Separation](#)

[ODHSOHA 090-003 Access Control Policy](#)

Contact

Office of Information Services

Service Desk

(503)945-5623

ois.servicedesk@odhsoha.oregon.gov

This process will be reviewed at least once every year to ensure relevance.

Process History

Version 1.0 DHS 1/10/06

Version 2.0 (Joint DHS|OHA) revised 10/28/2015

Version 3.0 ODHSOHA revised 08/02/2021

Version 4.0 ODHSOHA revised 12/04/2023

Keywords

Access, access control, Human Resources Management System, HRMS, Individual Access Request, IAR online 786, right of access, user access

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@odhsoha.oregon.gov