Office of Information Services
Information Security and Privacy Office

Process steps

Title:	ODHS|OHA 090-003-05 User Access Process
Related to:	ODHS|OHA 090-003 Access Control Policy
Effective date:	08/02/2021

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 adds, modifies, moves, or deletes 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|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. For individuals placed in our Human Resources Management Systems (HRMS), basic network access as approved by ODHS or OHA leadership are automatically granted when the individual is validated as an active ODHS|OHA individual in HRMS.
   a. Basic network access includes identity in the approved authorization system, access into agency computers and network, email, calendar and the ODHS|OHA Intranet.
   b. The remainder of these steps must be followed for all other system access. No other access is granted until step 1 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. (If offboarding, ensure the "effective date" is the last day of employment and skip steps 3.b. and 3.c.)
   b. Completes any necessary program specific forms for access to other systems in preparation for submission. (Certain 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. Programs requiring an exception to use the PDF version of the IAR 786 follow these steps:

    a. A manager with access approval authority submits the request to the OIS Service Desk.
    b. The OIS Service Desk forwards the request to the OIS Customer Services and Support (CSS) Director and Deputy Director.
    c. Decisions made by the OIS CSS Director or Deputy Director are communicated to the program manager.
5. Requests are automatically recorded in the OIS approved ticketing system.
6. OIS:
    a. Confirms with HRMS and Human Resources that the individual for whom access is requested is authorized for access to ODHS|OHA systems. This is not required for offboarding or for contractors and partners.
    b. Forwards the IAR 786 extract and the program specific form(s) 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/or 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
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. 5
Social Security Administration Information Exchange Security Requirements and Procedures
ODHS|OHA 090-003-06 User Access Process 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
Center for Internet Security Top Twenty Critical Security Controls
Statewide Information and Cyber Security Standards 2019

Forms referenced

IAR 786 Individual Access Request
MSC 0786 Network and Email New Individual Access Request

Related policies

DAS 107-004-052 Information Security
DHS 060-010 Background Checks
DHS 060-007 Employee Separation
ODHS|OHA 090-003 Access Control Policy

Contact

Office of Information Services
Service Desk
(503)945-5623
ois.servicedesk@dhsoha.state.or.us

Process History

Version 1.0 DHS 1/10/06
Version 2.0 (Joint DHS|OHA) revised 10/28/15
Version 3.0 ODHS|OHA revised 08/02/2021

Keywords

Access, access control, email, user identification, Human Resources Management System, HRMS, Individual Access Request, IAR online 786, MSC 0786, 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@state.or.us.