Process steps

Title:	ODHS|OHA 090-003-01 Privileged Access and Management Process
Related to:	ODHS|OHA 090-003 Access Control Policy
Effective date:	02/01/2021

Purpose

This process includes the steps for authorization, approval, and monitoring for an individual member of the Oregon Department of Human Services (ODHS) and Oregon Health Authority (OHA) staff, contractors, and partners who request privileged access.

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. Contractors and partners may face termination of the working relationship as well as federal sanctions.

Definitions

1. Privileged access: System access provides greater access to an individual than to the average end-user and enables the privileged user to take elevated actions to an information system that may affect computing systems, network communication, or the accounts, files, data, or processes of other users. Examples of privileged access include desktop administrator rights, server administrator rights, direct database access, application administration, etc.
2. Privileged access identity: A unique authentication name used only for administrative purposes.

Process Steps

1. To add or modify privileged access to ODHS|OHA information systems and applications, the requestor, an affected end user, manager, or designee, completes the DAS Individual's Privileged Access Request (IPAR) Form.
2. The requestor submits the completed IPAR form using Service Desk Online Individual Access Request (IAR 786) per the ODHS|OHA 090-003-05 User Access Process, which will create an OIS Service Desk request ticket.

a. For access as a server administrator, a current server administrator for that server submits the request.
b. For any other requests, the requestor submits the request.

3. Once the manager's approval is complete, OIS validates or creates the privileged access identity for the privileged access.
4. OIS transfers the approved tickets to the OIS Service Desk ticketing system work group "OIS Privileged Access".
5. The Privileged Access Authorized Approver (PAAA) validates an OIS technical manager has approved the privileged access. The PAAA:
   a. Checks that an approval from an OIS technical team manager is documented in the OIS Service Desk ticket.
   b. If not already approved, identifies an OIS technical team manager, obtains approval, and documents in the OIS Service Desk ticket.
6. The PAAA will:
   a. Validate an OIS technical team's director approval.
   b. If an OIS information technology (IT) technical director has pre-approved the team requesting access, the PAAA processes the privileged access request.
   c. If the individual is not on a pre-approved OIS IT technical director team, the PAAA contacts the appropriate OIS IT technical director for approval.
7. The PAAA documents the OIS Service Desk request.
   a. If denied, the PAAA updates and closes the OIS Service Desk ticket, automatically notifying the requestor of the decision.
   b. If approved, the PAAA:
      A. For the Department of Administrative Services (DAS) Data Center Services (DCS) privileged access requests, forwards an approval of the request via email with the appropriate forms attached to the DCS Service Desk and update the OIS Service Desk ticket.
      B. For OIS privileged access requests not managed by DCS, updates the OIS Service Desk ticket indicating approval, and transfers the ticket to the OIS Service Desk ticketing system work group for the appropriate technical team.
8. For requests to DCS:
   a. DCS verifies and processes the request and notifies the requestor and PAAA via email.
   b. The PAAA, upon receipt of completion, closes the OIS Service Desk ticket, automatically notifying the requestor.
9. For non-DCS requests, the assigned OIS technical team:
   a. Verifies the request.
   b. Processes and closes the OIS Service Desk ticket, automatically notifying the requestor and requestor's manager. Requestor confirms privileged access is available.
10. If there is a need to disable privileged access immediately:
    a. The individual manager or PAAA communicates with the appropriate Office of Human Resources staff who will contact the OIS Identity and Access Management group for action and disabling.

b. If the need to disable privileged access is related to a security incident, the Information Security and Privacy Office (ISPO) notifies the OIS Identity and Access Management group for action and disabling.

References

45 CFR 164
MARS-E Document Suite, Version 2.0, Volume III: Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges
Criminal Justice Information Services (CJIS) Security Policy
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 & Technology (NIST) Special Publication (SP) 800-53, Rev. 5
Social Security Administration Information Exchange Security Requirements and Procedures
Statewide Information and Cyber Security Standards 2019
ODHS|OHA 090-003-02 Privileged Access and Management Process Map
ODHS|OHA 090-003-05 User Access Process-Regular Employees
ODHS|OHA 090-003-06 User Access Process Map-Regular Employees

Forms referenced

DAS Privileged Access CIO Agreement
DAS Individual's Privileged Access Request Form
DAS Individual's Privileged Access Agreement
MSC 0786 Network and Email Individual User Profile (IUP) form

Related policies

DAS 107-027-010 Privileged Access to Information Systems Policy
DAS 107-004-110 Acceptable Use of State Information Assets
ODHS|OHA 090-003 Access Control Policy
ODHS|OHA 090-005 Security Incident Management Policy
OHA 100-008 Using the Minimum Necessary Standard for Individual Information

Contact

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

Process History

Version 1 DHS|OHA established 10/30/15
Version 2 DHS|OHA revised 03/06/17
Version 3 ODHS|OHA revised 02/01/2021

Keywords
Access, approver, authorized, Data Center Services, DCS, Identity and Access Management group, ID and Access group, PAAA, privileged, Privileged Access Authorized Approver

---