Process steps

Title:	DHS|OHA-090-003-01 Privileged Access and Management Process
Related to:	DHS|OHA-090-003 Access Control Policy
Effective date:	03/06/2017

Purpose

Privileged access enables an individual to maintain, administer, and troubleshoot the Department of Human Services (DHS) and Oregon Health Authority (OHA) information systems and applications. DHS|OHA shall comply and use the DAS-107-027-010 Privileged Access Policy, agreements and forms for privileged access to information systems managed by Enterprise Technology Services (ETS) and applications managed by DHS|OHA. This process includes the steps for authorization, approval, and monitoring for an individual (DHS|OHA staff, contractors, and partners) who requires privileged access.

Designation of Authorized Approvers

1. The Office of Information Services (OIS) Chief Information Officer (CIO) delegates certain OIS directors or managers to be Privileged Access Authorized Approvers (PAAAs) of privileged access requests for specific information systems and applications, and shall be maintained on a list available to the OIS Identity and Access Management group and ETS.
2. The OIS CIO or delegate shall complete and submit the DAS Privileged Access Customer CIO Agreement with the names of the PAAAs to the ETS Service Desk.
3. This agreement shall be reviewed on an annual basis, and updated as needed or when required.

Privileged Access Management

1. Approved requests shall be maintained in the service desk ticketing system for auditing purposes.
2. Privileged access account passwords shall be changed based on compliance requirements of the system.
3. Management and auditing of privileged access accounts shall be monitored through the privileged access report in accordance with compliance requirements for the specified system:
   a. Created by the specified system’s identity management and access management tools, and sent to designated staff.
   b. Archived according to the record retention rules and schedules, and compliance requirements of the specified system.
4. If there is a need to disable privileged access immediately:
   a. The individual manager or PAAA shall communicate with the appropriate Office of Human Resources who will then contact the OIS Identify 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) shall notify the OIS Identity and Access Management group for action and disabling.

Privileged Access Process Steps

1. To add or modify privileged access to DHS|OHA information systems and applications, the affected end user (requestor) shall:
   a. Request a new privileged access account for the requested domain through submission of the Network and Email Individual User Profile (IUP) MSC 0786 form in accordance with DHS|OHA-090-003-05. (This step must be completed prior to moving to step 1.b.)
   b. Complete the DAS Individual's Privileged Access Request Form and the DAS Individual Privileged Access Agreement Form.
   c. Send the request via email with the forms attached to the requestor's manager.
2. The requestor's manager shall:
   a. Review the request.
   b. Contact the server owner to obtain approval for the privileged access for the servers in question.
   c. Once approved, forwards the privileged access forms and the server owner's approval of the request via email to the OIS Service Desk.
3. OIS Service Desk creates a service ticket for IT Director's approval in the service desk ticketing system group "Access Approval-PA IT Directors ONLY".
   a. The IT Director indicates approval in the service ticket and transfers the ticket to the service desk ticketing system group "OIS Privileged Access".
   b. The PAAA reviews the request. (The requestor's manager shall be different from the PAAA.)
4. If denied, the requestor's manager notifies the requestor of the decision.
5. The PAAA reviews the request.
   a. If denied, the PAAA updates and closes the service ticket, automatically notifying the requestor of the decision.
   b. If approved, the PAAA either:
      A. For ETS privileged access requests, forwards an approval of the request via email with the forms attached to the ETS Service Desk and updates the service ticket.
      B. For OIS privileged access requests not managed by ETS, updates the service ticket indicating approval, and transfers the ticket to the service desk ticketing system group "CSS T2 ACCT PROV".
6. For requests to ETS:
   a. ETS verifies the request. ETS processes the request and notifies the requestor and PAAA via email.
   b. The PAAA, upon receipt of completion, closes the service ticket, automatically notifying the requestor.
7. For non-ETS requests, the OIS Identity and Access Management group:
   a. Verifies the request.
   b. Processes and closes the service ticket, automatically notifying the requestor and requestor's manager. Requestor confirms privileged access is available.

References

45 CFR 164

ORS 182.122

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. 4

SANS Institute

Social Security Administration Information Exchange Security Requirements and Procedures

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

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

DHS|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

DHS|OHA-090-002 Information System Audit and Monitoring Policy

DHS|OHA-090-003 Access Control Policy

DHS|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

Keywords

Access, approver, authorized, Enterprise Technology Services, ETS, Identity and Access Management group, ID and Access group, minimum necessary, PAAA, privileged, Privileged Access Authorized Approver, roles, Service Desk

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.