Operational Policy

Policy title:	Administrative Privileges Policy		
Policy number:	ODHS|OHA 090-013		
Original date:	03/07/2022	**Last update:**	03/07/2022
Approved:	Kris Kautz, Deputy Director OHA Don Erickson, Chief Administrative Officer ODHS		

Purpose

The Oregon Department of Human Services (ODHS) and the Oregon Health Authority (OHA) are committed to the security of agency information systems. The agency gives administrative access to limited numbers of individuals under clearly defined circumstances to reduce the risk of exposure to the ODHS|OHA network from malware and other vulnerability exploits that may lead to security incidents, system performance issues, lost productivity, higher support costs, and the unavailability or loss of data.

Description

This policy describes the circumstances under which administrative privileges are granted to ODHS|OHA staff and the on-going administration and monitoring of those privileges.

Applicability

This policy applies to all ODHS|OHA staff, including employees, 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.

Policy

1. Staff shall be provided only with the level of access necessary to accomplish assigned tasks in accordance with agency missions and business functions.
2. Staff with administrative privileges shall only use this elevated access when performing assigned tasks such as installing updates, installing applications, managing user accounts, and modifying operating system (OS) and application settings.
3. Staff with administrative privileges shall use a dedicated or secondary account for activities requiring elevated privileges. Users shall:
   a. Establish unique, different passwords for their administrator and non-administrative accounts.

b. Utilize multi-factor authentication and encrypted channels for all administrative account access. Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts shall use passwords unique to the system that meet any applicable regulatory requirements.
c. Only use agency supported equipment when performing tasks requiring administrative privileges.
d. Install only approved software on agency-owned devices.

4. ODHS|OHA shall use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure only authorized individuals have elevated privileges.
5. Management shall be responsible for monitoring administrative account access to ensure it is used appropriately and remains necessary to perform assigned job functions.
6. If services are outsourced to third parties, language shall be included in the contracts or in a standalone agreement to ensure the third party protects and controls administrative access and complies with any applicable federal requirements. The program sponsoring the access shall also submit a MSC 0785 Third Party Information System Access Request.

References

Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy
Internal Revenue Service Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies
National Institute of Standards and Technology (NIST) Special Publications (SP) 800-53 Rev. 5
NIST SP 800-114 Rev. 1
MARS-E Document Suite, Version 2.0: Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges
Statewide Information and Cyber Security Standards 2019
Statewide Information Security Plan
ODHS|OHA Agency Information Security Plan
Center for Internet Security Top Twenty Critical Security Controls
ODHS|OHA 090-003-05 User Access Process
ODHS|OHA 090-003-08 Third Party Entity Approval for System Access Process

Forms

MSC 0785 Third Party Information System Access Request

Related policies

DAS 107-004-110 Acceptable Use of State Information Assets
DAS 107-004-140 Privileged Access to Information Systems
ODHS|OHA 070-014 Information Technology Asset Management Policy
ODHS|OHA 090-003 Access Control Policy
ODHS|OHA 090-009 Administrative, Technical and Physical Safeguards of Information Policy

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

Contact

Office of Information Services

Service Desk: 503-945-5623
OIS.servicedesk@dhsoha.state.or.us

Policy history

Version 1 ODHS|OHA established 03/07/2022

Keywords

Access, account, administrative account, administrative rights, administrative privileges, configure, multi-factor authentication, password, privileges

---