Process

Title:	ODHS|OHA 090-003-015 Service Account Password and Management Process
Related to:	ODHS|OHA 090-003 Access Control
Effective date:	05/03/2021

Purpose

Service accounts are used for running application software or are used internally by the operating system. The purpose of this process is to outline the steps to obtain and manage a service account password for information technology (IT) system tasks for the Oregon Department of Human Services (ODHS) and Oregon Health Authority (OHA).

Applicability

This process applies to all ODHS|OHA staff including employees, volunteers, trainees, interns, as well as contractors and partners. This process applies to active directory only.

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.

Process Steps

1. A service account is a type of account that an application or server uses to interact with the operating system. A service account not designated as an individual user account.
2. Owners of service accounts accessing ODHS|OHA information systems follow these requirements for service account password assignment:
   a. Create passwords that meet complexity standards.
   b. Change service account passwords every 180 days.
   c. Restrict to specific devices and hours when possible.
   d. Assign permissions based on the principle of least privilege.
   e. Prohibit sharing service account credentials.
3. Passwords will be composed of the following:
   a. At least fifteen (15) characters long.
   b. At least one character from each of these categories:
      A. Uppercase letter (A-Z)
      B. Lowercase letter (a-z)

C. Numeral (0-9)
D. Special character (% @ # $! * / + > < [ ] { } \ -)

c. Passwords will not include spaces.
d. Passwords will not be set to one of the last 24 previously used passwords.

4. Exception requests for non-expiring passwords require a 64-character minimum password length and meet active directory complexity requirements. Regulatory compliance is the sole responsibility of the service account owner.
5. If a service account connects to cloud services, it requires a 64-character minimum password and meets active directory complexity requirements.
6. ODHS|OHA information systems and applications will not display passwords in plain text when entered and will not transmit unencrypted passwords.
7. The use of standalone Managed Service Accounts (sMSAs) and group Managed Service Accounts (gMSAs) are recommended for use by ODHS|OHA staff since the passwords are automatically generated.
   a. sMSAs are a type of domain account created and managed by the domain controller for use running a service.
   b. gMSAs provide the same functionalities as sMSAs, and extends that functionality over multiple servers.

References

Criminal Justice Information Systems Security Standards (CJIS)
IRS Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies
Group Managed Service Accounts, Microsoft
MARS-E Document Suite, Version 2.0, Volume III: Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges
National Institute of Standards and Technology (NIST) Security and Privacy Controls for Federal Information Systems and Organizations SP-800-53 Revision 4
National Institute of Standards and Technology Internal Report (NISTIR) 7966
Statewide Information Security Standards March 2017
ODHS|OHA 090-003-04 Managing Password Process
ODHS|OHA 090-003-08 Third Party Entity Approval for System Access Process
ODHS|OHA 090-003-015 Service Account Password and Management Process

Related policies

DAS-107-004-052 Information Security
DAS 107-004-110 Acceptable Use of State Information Assets
ODHS|OHA 090-003 Access Control Policy

Contact

Office of Information Services
Service Desk: 503-945-5623
DHS.ServiceDesk@state.or.us

Process History

Version 1 Established as DHS|OHA process 11/05/2018

Version 2 revised Joint ODHS|OHA 05/03/2021

Keywords

Access, account, controls, exceptions, group Managed Service Accounts, gMSAs, password, service, service account, standalone Managed Service Accounts, sMSAs

---