Operational Policy

Policy title:	**Password Policy**		
Policy number:	ODHS|OHA 090-014		
Original date:	10/04/2021	**Last update:**	10/04/2021
Approved:	Kris Kautz, OHA Deputy Director Don Erickson, ODHS Chief Administrative Officer		

Purpose

Passwords are the primary form of user authentication for granting access to Oregon Department of Human Services (ODHS) and the Oregon Health Authority (OHA) information systems. Compromised passwords remain the top cause of data breaches. To ensure that passwords provide as much security as possible, they must be carefully created and used. The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change.

Description

The policy outlines requirements for ODHS|OHA staff to implement and support agency expectations on the proper use and protection of passwords.

Applicability

This policy applies to all ODHS and 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.

Policy

1. Passwords shall be constructed according to set length and complexity requirements as noted in ODHS|OHA 090-003-04 Managing Password Process.
2. Specific password requirements for ODHS|OHA information systems shall be followed based on the platform (Mainframe and Windows platforms) and the type of data held within the system, such as Social Security Administration (SSA) and Criminal Justice Information (CJI).

3. When specific federal or system requirements are not applicable, staff shall follow the Information Security and Privacy Office (ISPO) and the Enterprise Information Services (EIS) Cyber Security Services (CSS) recommendations.
4. Temporary or default passwords shall be changed at the first successful login.
5. Agency information systems and applications shall not display passwords in plain text and shall only transmit encrypted passwords.
6. Staff shall only store agency passwords using secure and approved methods including browsers, websites, or password managers.
7. Staff shall use different passwords for each agency network and system account they utilize.
8. Staff shall keep their passwords confidential and avoid sharing unless required by a documented and approved business need.
9. When a system assigned password is issued or changed, or a password must be communicated for other system reasons, the password shall only be communicated securely via email or other forms of electronic communication and without other identifying information in the communication.
10. The use of administrator account passwords shall follow ODHS|OHA 090-013 Administrative Privileges Policy.
11. If an account or password is suspected to have been compromised, staff shall immediately:
    a. Change their password.
    b. Notify the Office of Information Services (OIS) Service Desk who then notifies ISPO.
12. Account access rights that are no longer needed shall be deleted or disabled immediately. This includes:
    a. When a user retires, quits, is reassigned, released, or dismissed.
    b. Contractor accounts, when no longer needed to perform their duties.
13. Multi-Factor Authentication (MFA), also referred to as Two-Factor Authentication (2FA) and Advanced Authentication (AA), is the most secure user authentication method currently available. Where applicable, staff using MFA shall be granted access after providing a minimum of two of the following:
    a. Something they know (personal identification number, password);
    b. Something they have (token, card, key); or
    c. Something that identifies them individually (fingerprints, facial recognition, retinal patterns).

References

45 CFR 160 General Administrative Requirements

45 CFR 164 Security and Privacy

Center for Internet Security Top Twenty Critical Security Controls

Center for Internet Security Password Policy Guide

Center for Internet Security MS-ISAC Security Primer-Securing Login Credentials

Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy

IRS Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies

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) Special Publications (SP) 800-53 Rev. 5

NIST Password Guidelines 2021

2019 Statewide Information and Cyber Security Standards

ODHS|OHA Managing Password Process 090-003-04

Office of Information Security Password and Credential Rules and Standard Version 1.2, June 19, 2020

InfoTech Research Group Password Procedural Policy

SANS Password Policy

Related policies

DAS 107-004-110 Acceptable Use of State Information Assets Policy

ODHS|OHA 090-003 Access Control Policy

ODHS|OHA 090-009 Administrative, Technical and Physical Safeguards of Information Policy

ODHS|OHA 090-013 Administrative Privileges Policy

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

Contact

Information Security and Privacy Office (ISPO)

Phone:503-945-6812 (Security)

OIS.policy@dhsoha.state.or.us

dhsinfo.security@state.or.us

Policy history

Version 1 Established 10/04/2021

Keywords

Account access rights, Advanced authentication, AA, default password, Multi-Factor Authentication, MFA, password

---