Operational Policy

Policy title:	Email Security Policy		
Policy number:	ODHS|OHA 090-015		
Original date:	02/07/2022	**Last update:**	02/07/2022
Approved:	Kris Kautz, Deputy Director, OHA Don Erickson, Chief Administrative Officer, ODHS		

Purpose

The purpose of this policy is to ensure the Oregon Department of Human Services (ODHS) and the Oregon Health Authority (OHA) staff are aware of and appropriately use email, while protecting against unauthorized data access and distribution, preventing the introduction of dangerous viruses, creating an opening for other security threats, data loss, and avoiding lost productivity.

Description

This policy outlines ways to ensure secure, safe, and effective use of email by ODHS and OHA staff.

Applicability

This policy applies to all ODHS|OHA staff, including employees, volunteers, trainees, interns, 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. ODHS|OHA staff shall protect the electronic transmission of confidential information, including protected health information (PHI), personally identifiable information (PII), Criminal Justice information (CJI), Federal Tax information (FTI), Payment Card Industry (PCI), and Social Security Administration (SSA) information.
   a. PHI includes any health information that can identify an individual including name, diagnosis, and medical record numbers. (Refer to OAR 943-014-0000(32))
   b. PII includes any information that identifies an individual, such as birth date, driver's license number, and financial account numbers.
   c. CJI includes all of the Federal Bureau of Investigations (FBI) Criminal Justice Information Services (CJIS)-provided data necessary for civil agencies to perform their mission.

d. FTI includes federal tax returns and return information (and information derived from it) received directly from the Internal Revenue Service (IRS) or obtained through an authorized secondary source.
e. PCI includes credit, debit, or other payment cards.
f. SSA includes Social Security numbers and their connection to specific individuals.

2. FTI shall not be sent via email or fax. If FTI is inadvertently emailed or faxed, staff shall follow the ODHS|OHA 090-005-01 Information Security Incident Reporting Process.
3. CJI shall only be transmitted via secure methods, such as secure file server or encrypted email.
   a. Recipients shall be CJIS-authorized staff.
   b. If CJI is transmitted unencrypted or to unauthorized staff, they shall follow the ODHS|OHA 090-005-01 Information Security Incident Reporting Process.
4. Email shall be used only for state related business. (Refer to DAS 107-004-110 Acceptable Use of State Information Assets for personal use exceptions)
5. Staff shall not forward emails containing sensitive, confidential, or protected information from their state email address to their personal email account.
6. Sending email or other electronic communications that attempt to hide the identity of the user or represent the user as someone else is prohibited.
7. Privacy incidents involving email shall be reported to the Privacy Help email box (DHS.PrivacyHelp@dhsoha.state.or.us) (Refer to OHA 100-014 Report and Response to Privacy and Security Incidents and ODHS|OHA 090-005-01 Information Security Incident Reporting Process)
8. Suspicious or suspected phishing emails shall be reported to ISPO by forwarding them to Bademail@dhsoha.state.or.us.
9. The email system is not an archiving tool and shall not be used for permanent storage of confidential or protected information. (Refer to ODHS|OHA 010-018 Record Retention and Management Policy)
10. All emails containing confidential information shall be sent securely utilizing approved encryption standards within the email environment.
11. Staff shall ensure that sensitive, confidential, or protected information is not included in the subject line of an email, including individual service recipient names.
12. Emails containing sensitive, confidential, or protected information in the body of the email or attachments shall only be sent to authorized individuals.
13. ODHS|OHA staff are responsible for understanding their data level of classification. (Refer to DAS 107-004-050 Information Asset Classification Policy)

References

45 CFR 160 General Administrative Requirements

45 CFR 164 Security and Privacy

OAR 943-014-0000 Privacy and Confidentiality

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

Microsoft Support Protect Yourself from Phishing

National Institute of Standards and Technology (NIST) Special Publications (SP) 800-53 Rev. 5

Minimum Acceptable Risk Safeguards for Exchanges (MARS-E) Document Suite Volume I: Harmonized Security and Privacy Framework Version 2.2

Statewide Information and Cyber Security Standards 2019
Statewide Information Security Plan
Center for Internet Security Top Twenty Critical Security Controls
ODHS|OHA 090-005-01 Information Security Incident Reporting Process
ODHS|OHA 090-005-02 Information Security Incident Reporting Process Map
Email Encryption for ODHS|OHA Employees (OIS Instructions)

Forms
MSC 2400 ODHS and OHA Policy and Procedure Summary

Related policies
Department of Administrative Services (DAS) 107-001-020 Public Records Management
DAS 107-004-050 Information Asset Classification
DAS 107-004-110 Acceptable Use of State Information Assets
ODHS|OHA 010-018 Record Retention and Management Policy
ODHS|OHA 090-005 Information Security Incident Management Policy
ODHS|OHA 090-009 Administrative, Technical and Physical Safeguards of Information Policy
OHA 100-014 Report and Response to Privacy and Security Incidents

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

Contact
Information Security and Privacy Office
Security: 503-945-6812
Fax: 503-947-5396
Dhsinfo.security@dhsoha.state.or.us

Policy history
Version 1 ODHS|OHA established 02/07/2022

Keywords
Electronic transmission, email, encryption, phishing, secure
