Operational Policy

Policy title:	**Administrative, Technical and Physical Safeguards Policy**		
Policy number:	DHS|OHA-090-009		
Original date:	11/08/2004	**Last update:**	02/05/2018
Approved:	Kris Kautz, OHA COO Dr. Reginald Richardson, Deputy Director DHS		

Purpose

The Department of Human Services (DHS) and Oregon Health Authority (OHA) are committed to protecting the information assets and systems of the agencies. The purpose of this policy is to establish criteria for safeguarding protected information and to minimize the risk of unauthorized access, use or disclosure.

Description

This policy describes the responsibility of DHS|OHA staff to maintain the security of information assets and systems during day-to-day workplace practices. This includes ensuring awareness of information that may be disclosed in documents and conversations, the security of workplace surroundings, the protection of information taken out of the work site, and the proper disposal of protected information.

Applicability

This policy applies to all DHS|OHA staff including employees, volunteers, 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. Contractors and partners may face termination of the working relationship as well as federal sanctions.

Policy

1. DHSIOHA shall take physical, technical, and administrative steps to protect information assets and systems from unauthorized access.
2. DHS|OHA shall protect agency-owned physical and electronic media including, but not limited to, the storage, accessibility, and transportation of protected information (personally identifiable information (PII), protected health information (PHI), federal tax information (FTI), Criminal Justice Information (CJI), or Social Security Administration (SSA) information.

3. DHS|OHA may monitor staff use of desktops, laptop computers, or mobile computing devices.
4. The Office of Information Services (OIS) shall provide secure installations, configurations, distribution, and management for all agency-owned information assets.
5. The Information Security and Privacy Office (ISPO) shall provide periodic training and reminders to DHS|OHA staff about information security and privacy best practices.
6. All members of the DHS|OHA workforce shall ensure that information assets and systems are adequately shielded from unauthorized disclosure by the following:
    a. Ensuring that portable computers or other media that store protected information have enabled encryption technology where technically feasible.
    b. Ensuring that information created or maintained in hard copy is safeguarded to prevent the possibility of unauthorized access. This includes the use of locking disposal containers to ensure the confidentiality of documents awaiting disposal or destruction.
    c. Ensuring that portable computers or other media that store confidential or sensitive information have enabled encryption technology.
7. DHS|OHA staff shall screen lock agency-owned or approved personal electronic devices, including computers, mobile communication devices, and other portable electronic devices if the devices are not in the area of the employee's immediate control.
8. DHS|OHA staff shall not use publicly accessible computers to access, process, store, or transmit protected information.
9. When using protected information away from the DHS|OHA work-site, staff shall comply with all work-site security requirements.
10. DHS|OHA staff shall not:
    a. Introduce any computer code designed to self-replicate, damage or otherwise hinder the performance of agency information assets or systems.
    b. Connect non-agency owned devices to any DHS|OHA network, with the exception of the guest network, without authorization from OIS.
11. Peripheral equipment such as printers, copiers, and fax machines that store, produce or transfer protected information shall be physically safeguarded from inadvertent or unauthorized access.
12. All email containing protected information shall be sent with #secure# in the subject line of the email. Federal Tax Information (FTI) shall not be transmitted via email.
13. DHS|OHA staff shall ensure that any fax containing protected information is prepared accurately and sent securely only to authorized recipients. FTI shall not be transmitted via fax.
14. DHS|OHA staff shall securely transport files and documents.
    a. DHS|OHA staff removing agency resources from the worksite, including protected information, hard copy files, agency laptops, mobile communication devices, and other portable electronic devices, shall assure the security of the resource.
    b. DHS|OHA staff authorized to remove protected information in hard copy from the worksite shall maintain physical custody and control of the documents or secure the documents in a locked environment.
15. DHS|OHA staff shall not post or share protected information about individuals on social media sites.
16. The Office of Information Services (OIS), through the Chief Information Officer (CIO) or designee, shall approve, control, and monitor as appropriate, local and non-local maintenance and diagnostic activities performed on DHS|OHA information systems.

17. In addition to the maintenance requirements, non-local maintenance, and diagnostic activities performed, authorized staff shall ensure:
    a. A level of security at least as high as that implemented on the system being serviced, including cryptographic mechanisms to protect the integrity and confidentiality of remote maintenance and diagnostic communications.
    b. Strong identification and authentication techniques such as multi-factor authentication in compliance with the requirements of the specified system.
    c. Encryption for secure communication in compliance with the requirements of the specified system.
    d. Privileged access management process for those authorized to conduct the remote maintenance and diagnostic activities as required.
    e. Remote maintenance capability is disconnected, including all sessions and network connections when maintenance activities are not being performed.
    f. Hardware is inspected and sanitized when taken offsite for maintenance or repair by non-state employees, and before reconnecting to the network.
    g. Password changes each maintenance session. as required by the security protocols of the specified system, if password based authentication is used.
18. For completed maintenance activities, audit logs shall be:
    a. Closely monitored and documented as required by the security protocols of the specified system.
    b. Archived following the record retention rules and schedules, and the security protocols of the specified system.
19. Digital and non-digital information system media shall be sanitized prior to disposal, released out of the agency's control, or released for reuse using defined sanitization techniques in accordance with applicable state and federal standards and policies.
    a. Sanitization mechanisms shall be employed with the strength and integrity equal to the security category or classification of the information.
    b. Hard-copy documents shall be finely shredded using approved equipment techniques capable of performing cross-cut shredding.
    c. Authorized personnel of the receiving entity shall be responsible for securing magnetic tapes or cartridges before, during, and after processing, and they must ensure that the proper acknowledgement form is signed and returned.
    d. Inventory records shall be maintained for purposes of control and accountability.
    e. Tapes containing protected information, any hard-copy printout of a tape, or any file resulting from the processing of such a tape shall be recorded in a log that identifies:
        A. Date received
        B. Reel and cartridge control number contents
        C. Number of records, if available
        D. Movement
        E. If disposed of, the date and method of disposition
    f. Surplus equipment shall be stored securely while not in use, and disposed of or sanitized.
20. DHS|OHA shall follow all applicable agency, state and federal law and requirements, the Department of Administrative Services (DAS) E-waste management guidelines, and DAS statewide policies.

References

Criminal Justice Information Services (CJIS) Policy

Federal Information Processing Standards (FIPS) Publication (Pub) 199

Federal Information Processing Standards (FIPS) Publication 200

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 Publication (SP) 800-53 Rev. 4

NIST SP 800-88

Social Security Administration Information Exchange Security Requirements and Procedures

2017 Statewide Information Security Standards

Department of Administrative Services e-waste Guidelines 07/26/17

45 CFR 160 & 164

OAR 125-055-0100 to 125-055-0130

OAR 943-014-0400 to 943-014-0465

DHS|OHA-090-009-01 Information System Maintenance Process

DHS|OHA-090-009-02 Information System Maintenance Process Map

Forms referenced

MSC 0785 Third Party Information System Access Request
MSC 0786 DHS|OHA Individual Access Request Form

Related policies

DAS 107-004-051 Controlling Portable and Removable Storage Devices
DAS 107-004-052 Information Security
DAS 107-004-100 Transporting Information Assets
DAS 107-004-120 Information Security Incident Response
DHS|OHA-010-014 Agency Compliance with Statewide Administrative Policy
DHS|OHA-070-014 Information Technology Asset Management Policy

OHA100-014 Report and Response to Privacy and Security Incidents

Contact

Information Security and Privacy Office
Security 503-945-6812
Dhsinfo.security@state.or.us

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

Policy history

Version 1 DHS 090-009 established 11/08/2004
Replaced by joint policy and renamed
Version 1 DHS|OHA-090-009 established 03/11/2015
Version 2 DHS|OHA-090-009 revised 03/04/2016

Version 3 DHS|OHA-090-009 revised 02/05/2018

Keywords
Administrative safeguard, authorization, access, disposal, email, federal tax information, FTI, individual, media, physical safeguard, privacy, protecting privacy, sanitization, security, safeguarding, technical, technical safeguard, transport, unauthorized

---