OREGON STATE HOSPITAL

PORTLAND – SALEM

POLICIES AND PROCEDURES

SECTION 1:	Administration	POLICY: 1.013
SUBJECT:	**Acceptable Use of Information-Related Technology**	
POINT PERSON:	DAN PASCH DIRECTOR TECHNOLOGY SERVICES	
APPROVED:	GREG ROBERTS SUPERINTENDENT	DATE: DEC. 2, 2011

I. POLICY

Oregon State Hospital has adopted DHS Policy AS-070-004, Acceptable Use of Information – Related Technology. (See attached)

Replaces OSH Policy and Procedure 1.013, *Internet Access for OSH Employees,* dated 6/28/2008.

DHS Policy
Oregon Department of Human Services

Administrative Services

Policy Title:	**Acceptable Use of Information-related Technology**				
Policy Number:	**DHS-070-004**	Version:	**1.0**	Effective Date:	12/10/2004

Approved By: *DHS Chief Administrative Officer* Approved Date: *12/10/2004*

Policy | Procedures | Forms, etc. | References | Definitions | Contact | History

Overview

Description: This policy outlines acceptable uses of DHS information-related technology. This includes, but is not limited to, all present and future forms of hardware, software, and services for data processing, and office automation (including e-mail, networks, Internet, printers, and other computing devices and applications).

Purpose/Rationale: Information-related technology is provided to automate business processes used within DHS, including workflow, access to and storage of information, communications, research, and more. Information-related technology investments shall be reserved for DHS business, with minor exceptions as noted.

Applicability: All individuals who have been granted access to DHS information-related technology or systems, including but not limited to full- and part-time employees, contractors, temporary workers, those employed by others to perform DHS work, and others with approved access are covered by this policy and shall comply with this and associated policies, procedures, and guidelines.

Failure to Comply: Failure to comply with this policy and associated policies, standards, guidelines, and procedures may result in disciplinary action up to and including dismissal from state service for employees or termination of contracts for contractors, partners, consultants, and other entities. Legal action also may be taken for violations of applicable regulations and laws.

Back to top

Policy

1. General

a. Installations shall be controlled. All installations of information-related technology within DHS shall follow department policies and procedures. (See DHS agency-wide policies: http://www.dhs.state.or.us/policy/)

b. Information-related technology and systems are for DHS business only. Except as allowed under this policy, systems shall be used only for the business of DHS as defined by DHS through its managers and supervisors.

c. Systems and information are state property. All systems and information are, and shall remain, the property of DHS, subject to its sole control. No part of DHS systems or information is, or shall become, the private property of any system user. DHS owns all legal rights to control, transfer, or use all or any part or product of its systems. All uses must comply with this policy and with all other department and state policies and rules that apply. Nothing in this policy limits any rights of DHS to control its systems, their uses, or information.

d. DHS has full control and access to information.

A. Control. DHS reserves, and intends to exercise, all rights relating to information used in its systems.

i. DHS intends to trace, review, audit, access, intercept, block, restrict, screen, delete, recover, restore, publish, or disclose any information, in accordance with applicable disclosure of information policies.

ii. DHS may withdraw permission for any or all personal or business uses of its systems at any time without cause or explanation.

iii. No one shall grant access to systems without DHS authorization. All access shall initially default to "denied." Access shall be granted as needed.

B. Access. Scramblers, encryption methods, re-mailer services, drop-boxes, or identity stripping shall not be used without DHS approval, access, and control.

i. No user shall attempt to access another user's account without DHS authorization.

ii. No user shall use DHS systems to attempt unauthorized access to any information or other system.

e. Public records are controlled by DHS. All system administrators and users shall comply with public record retention laws and rules, including records that are contained in electronic form (i.e. electronic files, data, e-mail, and other forms of electronic communications).

A. DHS reserves sole discretion to decide what information is a public record.

B. DHS may disclose any public record without permission or knowledge of any systems user.

C. *Except as noted in this policy, users may not expect that any personal use of DHS systems will be private or privately owned.*

f. Uses must reflect the department image. Uses do not all have to be formal; but they must be professional.

g. Uses must be lawful and inoffensive. Uses of DHS systems must not be false, unlawful, offensive, or disruptive.

A. Unless DHS duty requires it, no use shall contain profanity, vulgarity, sexual content, or character slurs. No use shall make inappropriate reference to race, age, gender, sexual orientation, religious or political beliefs, national origin, health, or disability.

B. Copyrighted or licensed information shall be used only with full legal right to do so. For example, this policy requires that individuals using commercial software must honor the licensing agreements that govern the use of that software.

2. Security

All use shall protect the technology and DHS information from risk, comply with policies, laws, and regulations, and reflect an acceptable image of DHS thus ensuring the confidentiality and availability of information.

3. Electronic Publishing

a. All electronic publishing is restricted to DHS business as defined by DHS. All publishing requires DHS authorization. Publishing means using systems to disseminate or spread information to the public or beyond the user's area of authority within DHS. Examples include newsletters, Web pages, fliers, chain letters, e-mail broadcasts, and postings to Internet groups or to e-mail lists.

b. Internal publishing of employee events is a mixed state and personal

business and must be authorized by DHS. Examples include charitable drives, retirements, parties, or whatever the agency deems suitably related to DHS business.

4. Web Use

a. Use of Web technology. All use of Web technology shall comply with this policy, DHS security policies, and any other DHS policies, procedures, and guidelines relating to the Web.

b. Review of Web content required. All published Web content shall be restricted to DHS business as defined by and through DHS management. All content must be reviewed by a program supervisor or manager prior to publishing. Published content must follow communication guidelines and standards as established by DHS.

c. Posting/publishing on Web. DHS, through supervisors and managers, may authorize a user to post (publish) queries or represent DHS by posting professional comments to useful groups. Comments must conform to this policy. Content and frequency of posting must reflect the interest of DHS, not the user.

d. Ordering goods through Web. Personnel authorized to make payment by credit card for goods ordered through the Web are responsible for the safe and appropriate use of the Internet.

e. Downloads from Web:

A. Downloads of business-related information is acceptable.

B. Downloads of applications or programs must be authorized by the supervisor and approved by OIS through DHS-070-007-02, Standards Exception Procedure.

C. Downloads that would update existing software must be authorized through OIS. Contact the OIS Help Desk.

f. Establishing new business channels via the Web: DHS Web connections shall not be used to establish new business channels without prior DHS authorization through DHS-070-014-03, Request to Connect to DHS Network Backbone (by Non-DHS Organization) Procedure. Examples include electronic data interchange (EDI) arrangements, electronic malls with on-line transactions, on-line database services, etc.

5. Personal Use

a. Personal use of DHS technology is permitted on a limited basis for incidental purposes.

A. Inappropriate examples: Uses requiring substantial expenditures of

time, uses for profit, or uses that would otherwise violate DHS policy.

B. Appropriate examples: Limited Web searches for personal research, self-study, and preparing a resume or application for a state job.

b. DHS has sole discretion to determine whether a use is personal or business or if it is incidental use.

c. Acceptable mixed use of state and personal use may be permitted at times as approved by the supervisor.

A. Examples include: Creating and printing a state job application, a resume, personnel and benefits papers, necessary materials for state-paid courses of study, or special event notices such as retirement announcements.

d. Any personal use:

A. Must conform to other sections of this policy.

B. Must take place during rest or meal breaks.

i. Not allowed before, after, or during work.

ii. Exception: Incidental, personal use of e-mail is permitted outside of breaks.

C. Must be limited, incidental, and minimal. The use should not be excessive or a part of a daily plan. When in doubt about what constitutes excessive use for personal business, ask your supervisor or contact the DHS Office of Human Resources.

D. Must be at virtually no cost to the state. The cost of personal use must always be minimal compared to use for assigned work.

E. Must not include installing, downloading, or executing personal software. This includes no-cost, non-licensed software.

i. Unacceptable example: User-supplied or Web downloads of screen saver software are not allowed. Only the screen saver software supplied with the operating system of the desktop is allowed.

ii. Acceptable example: Minimal, limited quantity of personal files placed on the local hard drive only, not on network drives. Files must comply with all other use and security requirements, i.e. no security risk, non-offensive, non-interfering with others or desktop operation.

F. Must not include connecting privately owned devices to the DHS

network or other DHS devices without proper authorization.

G. Must not include any system or device that the user does not employ in his or her assigned work. DHS-owned system devices taken home remain subject to this policy.

H. Must not adversely impact the capacity of or cause a security risk to information-related technology systems.

   i. Adverse impact on system capacity: When someone accesses/listens to radio channels or views videos over the Internet. These activities are not allowed.

   ii. Adverse security risk: Downloads of files not scanned for viruses or an executable file downloaded to the desktop or network drives without authorization.

I. Must not include accessing non-secure, personal Web-based accounts.

J. Must not include instant messaging technology for personal communications.

K. Must not include playing computer games, whether Internet, personal, or those included within approved software applications.

L. Must not be for or on behalf of any organization or third party.

M. Must not include publishing personal content to the Web. This bars personal web pages, personal postings to Internet groups, chat rooms, web pages, or list services.

N. Must not include soliciting, lobbying, recruiting, selling, or persuading for or against commercial ventures, products, religious or political causes, outside organizations, or the like.

O. Must not interfere with others' ability to work, i.e. headphones are required for audio devices, or the volume must be kept low enough not to be heard outside the employee's immediate work area.

P. Must not include creating, sending, or forwarding junk mail or chain letters.

Q. Must not include activities that result in personal gain.

R. Must not be for political purposes.

6. Union Use

Refer to union contract for negotiated allowable uses of information-related technology, such as use of the DHS e-mail system.

Back to top

Procedure(s)

- DHS-070-007-02, Standards Exception Procedure
- DHS-070-014-03, Request to Connect to DHS Network Backbone (by Non-DHS Organization) Procedure

Back to top

Form(s)

- None

Back to top

Reference(s)

- Frequently Asked Questions - Acceptable Use of Information-related Technology
- Guidelines - Email Etiquette
- Guidelines - Email System Use
- DHS Administrative Services Information Technology policies
- DHS Administrative Services Information Security policies
- DHS Agency-wide Policies
- Department of Administrative Services (DAS) Oregon Statewide IT Policies
- Oregon State Agency General Records Retention Schedules

Back to top

Definition(s)

- See Common Terms for DHS information technology policies
- See Common Terms for department-wide support services policies

Back to top

Contact

- **Name:** Janet Gerling; **Phone:** 503-945-6244; **Email:** janet.m.gerling@state.or.us

Back to top

Policy History

- **Version 1.0:**
  - 12/10/2004 - Initial Release (Supercedes AS-070-011, version 2.0, Internet Use policy)

Back to top

If you have comments about this site, send email to dhs.policyinfo@state.or.us.

Oregon Department of Human Services
500 Summer St. NE E25, Salem, OR 97301-1098
Phone: (503) 945-5944
Fax: (503) 378-2897
TTY: (503) 947-5330