SCHOOL OF DENTISTRY
UNIVERSITY of WASHINGTON

Information Security

USER'S GUIDE

May 2009

Information Security is the responsibility of all users.

Information Security is not just about computers, it is how we go about our business at the School of Dentistry. We have a set of standards and policies that define our Information Security requirements, and we all must follow them.

Report Information Security Incidents or ask questions about your computer's security by calling The Help Desk: 206-616-3591

University of Washington Policies

Reminder: We are all part of the University of Washington and we are required to follow UW policies.
http://depts.washington.edu/uwcopy/UW_Policies/

Your Accounts, Privileges, and Passwords

Don't share your user ID, logins and/or passwords (this includes logging in for others) even if you do not use confidential information.

Accountability

You will be held accountable for all activities associated with the use of your individual user accounts and related access privileges.

Restrict Your Use

Washington State Law restricts our use to authorized duties or activities. Authorized duties or activities are established by those with appropriate authority related to your role or function, such as a supervisor, manager, administrator or chair.

Classification of Information

Confidential Information is information that is very sensitive in nature and requires careful controls and protection. Examples include: Protected Health Information, student records, social security numbers and passwords.
Restricted Information is less sensitive than confidential information, but this data should only be shared with School of Dentistry workforce on a need-to-know basis. Examples include: business plans, intellectual property, financial information or other sensitive materials.
Public Information is either approved for general access, or by its very nature is not necessary to protect, and can be shared with anyone.
You are expected to safeguard all Restricted and/or Confidential information.

Secure Disposal Restricted & Confidential Information

Secure disposal usually means reducing to very small particles (e.g., shredding) that cannot be reconstructed or used in any combination to recreate the original.

Disclosure of Restricted & Confidential Information

- Don't allow others to use your access to restricted and/or confidential information.
- Don't disclose/share restricted and/or confidential information unless it is part of your job functions.
- If disclosing/sharing restricted and/or confidential information is part of your job, make sure you only share the necessary information with the appropriate persons.

Clear Workspace

Outside of normal working hours, put away RESTRICTED and/or CONFIDENTIAL information in your workspace. Examples: Storing paper and computer media in suitable locked cabinets or desks when not in use or when unattended, picking up print jobs immediately and protecting fax machines from unauthorized access.

Secure Your Workstation

- Terminate computing sessions or lock workstations when not in use or when unattended.
- Log-off networked systems when the computing session is finished.
- Protect workstations in public areas so PHI is not visible to patients or other unauthorized individuals.

After Hours

- SOD PCs are required to be locked and powered on (not shut down) after hours.
- Otherwise follow the direction of those responsible for your computer support.

Physical Space Security

- Use appropriate measures such as locked doors.
- Question individuals without ID badges.
- Make sure that vendors check in and are escorted in your department.

Use your Anti-Virus

- If you access files on mobile media, such as diskettes & thumb drives, use anti-virus software to scan files before using them on another computer (SOD computers are set to perform a virus scan when a file is accessed from any device).
- Don't open email attachments from unknown senders.
- Verify attachments from known senders and scan them before opening.

Do Not Change the Computer Configuration or disable or alter anti-virus or Firewall

"Computer Configuration" refers to the combination of hardware, software, operating system, and the settings used to set up each of these items. These settings apply to all users of the system and are not changeable except by someone with elevated privileges. Examples of computer configuration are operating system settings, firewall settings, system time, and installed applications that require a change to the system set-up. Alteration of these could introduce security risks or damage/disable a computer if not done properly. Do not change computer configuration unless specifically approved by IT/Computer Support.

Do Not Download, Install or Run Unknown Files or Software

Today's computing environment is incredibly hostile. The number of worms, viruses, and spy-ware has skyrocketed. It is School of Dentistry policy that:
Only designated system administrators are to install software, **and**
Only licensed and authorized (System Owner approved) software is used.

Use of Departmental Computers

Aside from *occasional* and *de minimus* (of minimal cost to the State) use, the personal use of computers, email and the Internet is prohibited. This limitation is similar to permitted personal use of non-computing resources, such as telephone calls. Washington State law also prohibits the use of UW computers for personal business-related, commercial, campaign or political purposes, or to promote an outside business or group or to conduct illegal activities. Additionally, employees are prohibited from allowing any member of the public to make personal use of state computers and computing resources. ***Washington State specifically prohibits use of UW computers for all political and commercial activities.***

Although de minimus personal Internet use is now allowable, many Internet activities are still prohibited. Downloading copyrighted files, such as MP3 music files, may violate copyright law and expose UW and you to penalties and fines. Internet activities can be traced back to your computer. Other examples of improper or excessive use are included in the Executive Ethics Board web site http://www.ethics.wa.gov/RESOURCES/FAQ.htm and the UW Administrative Policy web site http://www.washington.edu/admin/adminpro/APS/47.02.html

Comply With Copyright Law

- Unauthorized use of software, images, music, or files is regarded as a serious matter and any such use is without the consent of UW School of Dentistry.
- If abuse of computer software, images, music or files occurs, those responsible for such abuse may be held legally accountable as well as be held accountable for violation of UW Policy.
- It is against UW policy for workforce members to copy or reproduce any licensed software except as expressly permitted by the software license.

Taking School Of Dentistry Equipment from the Premises

1. Obtain authorization to take equipment offsite.
2. Log out the equipment.
3. When returned, log the equipment back in.
4. Be aware of department expectations about off-site use of equipment.
5. Secure the information with controls comparable to those of equipment on-site.

Computing Devices Connected to the School Of Dentistry Network

Computing devices connected to the SOD network must meet these minimum Information Security requirements:

1. Terminate computing sessions or lock workstations when not in use or when unattended.
2. Approved operating system that is patched in a timely manner.
3. Protection against malicious software (i.e. anti-virus protection).
4. Filtering or firewall protection.
5. Enabled logging and auditing.
6. Approved network media & protocols.

Reusing Electronic Media

If the electronic media had RESTRICTED and/or CONFIDENTIAL information there are 2 approved methods:

1. **Overwriting method** Overwriting uses a software program to write (1s, 0s, or a combination) onto the media. (hard drives & floppy disks)
   Overwrite the media a minimum of three times.
2. **Degaussing method** magnetically erases data from magnetic media. (magnetic tapes)

Auditing & Monitoring

Heads Up! School of Dentistry and UW Medicine monitor and audit to assure appropriate access.

Sanctions

School of Dentistry has sanctions for the failure to follow policy and/or for a breach of patient confidentiality or information security. The School applies appropriate sanctions against individuals for failure to comply with the security policies and procedures that are based upon our security policies.

Key Terminology

Protected Health Information (PHI) –
PHI includes every single element of individually identifiable health information that is maintained in permanent health records and/or other clinical documentation in either paper-based or electronic format. PHI is an example of a CONFIDENTIAL classification.
Safeguard - Protect or cover from exposure, using precautionary measures, usually by keeping the information in the strictest confidence.
System Owners - Individuals within the School of Dentistry community accountable for the management and use of one or more electronic information systems, electronic databases, or electronic applications.
Workforce - Faculty, employees, students, trainees, volunteers, and other persons who perform work for School of Dentistry, and whose work conduct is under the School's control regardless of whether or not they are paid by the School.

Resources:
School of Dentistry HIPAA Security Policies (adopted from UW Medicine):
http://dental.washington.edu/compliance/hipaa/

School of Dentistry Compliance Website:
http://dental.washington.edu/compliance/

School of Dentistry Director of Compliance & Privacy:
206-543-5331 or box 356365