Computer Support Guidelines

http://www.washington.edu/computing/security/responsibilities.html states the following general usage guidelines for the UW computer users:

**As a Computer User:**

- Read, understand, and follow all related UW policy and guidelines.
- Never use UW Computing resources for any illegal, unauthorized or unethical act as defined by law or UW standards of conduct.
- Protect and never share your password or UW NetID. Remember you are accountable for all activities associated with your account.
- Never share your computer accounts and access privileges assigned to you or others. Access privileges are assigned based on a person's specific requirements for using UW computer and network resources. The ability for the UW to protect its electronic records and systems depends on access control measures.
- Always restrict your use of UW computer systems, networks, email, and Internet privileges to authorized and appropriate uses.
- Always save sensitive information on a well-managed and well-protected server.
- Saving sensitive information on a desktop machine is not appropriate in most circumstances.

UW Tacoma has the following additions to the UW guidelines:

**In General:**

Laptops and Desktop computers purchased by UW TACOMA and for use by UW TACOMA personnel (collectively called “UW TACOMA-owned computers”) are configured prior to delivery to allow access to the campus network. This connection must be kept intact and capable for the service life of the UW TACOMA-owned computer.

All UW TACOMA-owned computers are properly configured and connected to connect to the UW TACOMA network and automatically obtain virus scanner updates and security patches. Computers not owned by UW TACOMA must have up-to-date virus scanning and security patches before connecting to the network. All end users of any computer must check that their computers are actively scanning for viruses. If training is needed, end users should submit a request to “Tachelp@u.washington.edu” or the IT Help web page (http://www.tacoma.washington.edu/it/help/). As a member of University of Washington, you can also use the free anti-virus scan software made available by Computing and Communications in Seattle. You can use the UWick kit CD-Rom or go to the web link (http://www.washington.edu/computing/software/sitelicenses/virusscan/) to find the free software and download information.

All authorized users of UW TACOMA-owned computers and the network are given a personal network drive for saving data (this is copy one). The F:, H:, and S: drives are for this purpose. These network drives are maintained by Computer Services and backed up to tape on a regular basis (copy two). If the end user wants an additional copy of critical data, Computer Services can add a storage device to individual computers as requested. It is the responsibility of the end-user to assure this third copy is in sync with the data located on the servers (copy one). The installation and materials cost incurred will be the responsibility of the requesting department. It is the responsibility of the end users to obtain training and ensure proper use of the storage device.

In the event that a UW Tacoma computer has a fatal error, it is assumed that all data and programs on the computer are lost. The Computer Services technician working on the problem will try to minimize data loss. If the computer requires a system restore, it will be rebuilt with a UW Tacoma standard image. Any special programs previously installed by Computer Services will be reinstalled, if possible. Due to newer versions of software and operating systems, the reinstallation of older versions of software may be problematic. Computer Services will decide if all the previously installed programs can be reinstalled on this computer. Computer Services will work with individual Program Directors and the end-user to decide how to rebuild the computer on a case by case basis.

**For Desktop computer users**

UW Tacoma-owned desktop computers must be powered on at all times. Computer Services requests that all end-users turn off their monitors and peripheral equipment before the end of each working day.

**For Laptop computer users**

UW Tacoma-owned laptop computers slated for office use should be placed in a location where they can be left in a powered on state with power-saving disabled and connected to the UW Tacoma network. Computer Services can provide assistance in obtaining the required hubs and power strips for this purpose.

If the laptop is disconnected from the UW Tacoma network for more than a week, users must run operating system security updates and antivirus updates weekly while connected to the network. For Windows laptop users, use Microsoft's updater (www.windowsupdate.microsoft.com), while Apple laptop users running OS X should use the Software Update feature.

Prior to check out or using a UW Tacoma laptop, the end user must complete a training or refresher course with a qualified UW Tacoma Computer Service technician or other person designated by Computer Services to conduct this training.