Definitions

Workstations: Includes faculty and staff laptops or desktops. They can be Windows, Mac or Linux devices. Linux is not a University-supported operating system.

Mobile Devices: University-owned mobile devices, such as tablets or smartphones, which can access the internet, store University data, and/or send or receive email from the University enterprise email system.

Responsibility for Secure Computing

Every individual is responsible for practicing secure computing when using the University's shared resources like email and the Internet. You are required to follow the instructions below to help you practice secure computing, protect your workstation from viruses, spam, and hackers and to make certain that you are able to pass an internal workstation/desktop security audit. If you have questions regarding implementing secure computing on your workstation please call the IT Service Desk at 801-626-7777.

Requirements for Secure Computing

Basic Operating System Requirements

All University-owned workstations are required to have an approved operating system version.

All computers storing sensitive information are to be encrypted using approved encryption software.

Perform Operating System Updates Regularly

Update and patch your operating system software to the most recent levels by configuring the operating system to automatically download and install Operating System security software updates. ***(If you have an older Operating System (OS), check with the IT Service Desk to verify that it is a University-supported OS version).***

Install and use a Firewall

All University-owned workstations must have a host-based firewall turned on. It is recommended that all workstations also have McAfee's Host Intrusion Prevention (HIPS) installed. The IT Service Desk can assist you with installing HIPS.

Install Antivirus and Anti-Spyware Software

All University workstations, labs, and mobile devices must use the University-approved virus scan software running with current DAT files and anti-spyware software.

All workstations and labs must install the management policy tool that is used to manage the antivirus and anti-spyware software. The IT Service Desk can assist you with installing the management tool if you do not currently have it installed.

Automatic Logins

Automatic logins must be disabled on workstations.

Lock Your Computer

All workstations must have the screen saver auto-lock feature enabled. The recommended amount of idle time for this feature is 10 minutes and must not exceed 20 minutes.

In areas where the workstation is visible or accessible to the public, users using those workstations must manually lock the workstation if left unattended. Instructions to manually lock your workstation are found on the Information Security Office website.

Confidentiality and Privacy of Information

Faculty and staff are expected to respect the confidentiality and privacy of individuals whose records they access. It is the responsibility of WSU employees to maintain the confidentiality of data they access or use and are responsible for the consequences of any breach of confidentiality.

Appropriate Use and Selection of Passwords

Passwords are the keys to all online resources. Everyone who connects to Weber online resources is responsible for taking appropriate steps to secure their accounts and select strong passwords. If two people share the same computer, each individual must have their own Profile, UserID, and password to access the computer.

Use Strong Passwords – A password is at least 8 characters long and is a combination of upper and lower case letters and numbers. Strong passwords do not include phrases, names, or other types of dictionary words.

Passwords *must not be y*our Wildcat Username, your name, or a word found in a dictionary.

You should never write down your password in an accessible or visible location or give it to anyone else.

You should never provide your password over the telephone.

You should never put your password in e-mail (even to University IT or technical support staff).

Disable Inappropriate Windows Components

Disable **Internet Information Services** (**IIS**). (IIS allows internet-based services for servers using Microsoft Windows such as Web and FTP support along with support for FrontPage, transactions, Active Server Pages, and database connections.)

Disable Network Services **Peer-to-Peer (P2P).** (P2P allows any peer-to-peer networking services and configures the Windows firewall to allow peer-to-peer networking connections.)

File & Printer Sharing Firewall Exception

Disable the **"**File and Printer Sharing" firewall exception**.** This exception allows the sharing of files and printers on computers with others on the network. (This component, when enabled, poses a security risk if the user has not adequately protected their files with a local firewall and appropriate authentication/authorization mechanisms.)

Licensed Software

All software used must have a proof of purchase and licensing. It is the user and/or departments' responsibility to maintain license documentation. For additional information please reference http://www.weber.edu/software/Ethics.html.

WSU Acceptable Use Policy (PPM 10-2)

All users must be familiar with and understand the requirements of the WSU Acceptable use Policy (http://www.weber.edu/ppm/Policies/10-2_AcceptableUse.html).

Exceptions to this Standard

Exceptions from this standard must be approved by the Information Security Office based on academic or business need. The exceptions will be brought before the Information Security Task Force for review. If the need for the exception no longer exists the Information Security Office is to be notified.

Exception requests can be made through the ISO website, www.weber.edu/iso.