

**Best Practices for Windows-based Desktop PCs on the Washburn Network**

<p><b>Ensure that your files are backed up and secure.</b></p>	<ul style="list-style-type: none"> <li>• Always save files on network drives.</li> <li>• Never save files on the desktop.</li> <li>• Never save files on the local drive (C:)</li> </ul>
<p><b>Ensure that your profile settings are saved and provide for nightly updating of files.</b></p>	<p>Each evening:</p> <ol style="list-style-type: none"> <li>1. Log out of your PC.</li> <li>2. Power off the monitor or make sure sleep mode is configured on your PC.</li> <li>3. Keep your PC powered on.</li> <li>4. If you know there is going to be a bad storm, power the machine off.</li> </ol>
<p><b>Ensure a better user experience and return Windows back to its original state.</b></p>	<p>Reboot your PC at least once a week:</p> <ol style="list-style-type: none"> <li>1. "Shut down" the PC. (This will power your PC off.)</li> <li>2. Wait 15 seconds.</li> <li>3. Power the PC on.</li> </ol>
<p><b>Comply with WU Acceptable Use Policy.</b></p>	<p><b>Never give your PC password (or any other password) to anyone else.</b></p>
<p><b>Decrease the likelihood that your account will be hacked.</b></p>	<p>Use passwords that are impossible to guess:</p> <ul style="list-style-type: none"> <li>• Use non-personal information. Avoid dates, family names, pet names.</li> <li>• Use words that do not appear in the dictionary. "Cat" or "dog" is bad, but "Catdog" would be good.</li> <li>• Incorporate a number or other symbol in your password. "Catdog" is good; "Catd06" is better.</li> <li>• Change your passwords frequently.</li> <li>• Use different IDs/passwords for distinct systems. (For example, do not use your bank PIN for your PC password.)</li> </ul>
<p><b>Protect your identity.</b></p>	<ul style="list-style-type: none"> <li>• Never respond to e-mail asking you to send a password, social security number or other sensitive info.</li> <li>• Use secure Web sites whenever sharing private information.</li> <li>• Learn about how Web sites use "cookies" to store information about you.</li> </ul>
<p><b>Protect your files.</b></p>	<ul style="list-style-type: none"> <li>• Lock your screen when you are away from your desk.</li> <li>• Avoid storing personally identifiable information on portable media (such as portable USB drives).</li> <li>• Use secure file transfer to encrypt your files in transit.</li> <li>• Establish secure connections with other machines to encrypt your login credentials and exchange of information.</li> </ul>
<p><b>Protect your computer from viruses and spyware and yourself from spam.</b></p>	<ul style="list-style-type: none"> <li>• Keep anti-virus features turned on.</li> <li>• Scan every file you receive for viruses, including files on removable media.</li> <li>• Do not open attachments unless the e-mail is from someone you know.</li> <li>• Keep automatic operating system updates running.</li> <li>• Keep anti-spyware software running.</li> <li>• Set up your Washburn E-mail filter quarantine.</li> <li>• Don't enter sensitive or financial information into pop-up windows.</li> <li>• Do not respond to e-mail messages giving you the opportunity to opt out. (This lets the spammer know you are alive and well!)</li> <li>• Download files only from trusted sites. Click on hyperlinks in e-mail ONLY if you trust the site.</li> <li>• Know that browser spoofing presents sites that appear to be trusted sites but are not.</li> </ul>
<p><b>Ensure that you will be able to reach Washburn Web resources.</b></p>	<p>Make washburn.edu a trusted site in your browser.</p>
<p><b>Prolong the life of your monitor.</b></p>	<p>Use setting for low-power sleep mode during periods of inactivity.</p>

**Questions? Visit [support.washburn.edu](http://support.washburn.edu) or e-mail [support@washburn.edu](mailto:support@washburn.edu).**