UNIVERSITY OF OREGON

Security Checklist

University of Oregon Administration

As employees of the University of Oregon we are privileged to have access to a fast, efficient computing system to assist us with our jobs. Part of our jobs is taking personal responsibility for keeping our computer and the information stored on it safe.

Just as you would lock your office when you leave, you should be taking basic steps to protect your computer from intrusion.

As administrators we have an even larger charge and that is to be sure our employees are practicing safe computer usage. Even one computer that does not follow basic safety standards can put an entire network at risk. Work with your IT support staff to institute policies and procedures to keep risk at a minimum. In addition, there are standard practices we can follow to make sure our department's systems are safe.

Adhere to the Basic Standards - Refer to the *Security Checklist for Computer Users*. Are you practicing these rules and setting a good example?

Acceptable Use – Be sure your employees are provided with a printed copy of the acceptable use policy in writing. http://cc.uoregon.edu/policy/acceptable_use.html.

Password Protection Policies - Your employees' passwords are their first line of defense for your systems.

- ✓ Be sure they are following the password standards provided in the *Security Checklist for Computer Users* document.
- ✓ Institute a password expiration policy for internal systems. Passwords should be changed every 6 months for optimal security.

Everyday Computer Protection – Many of us work with sensitive information on a daily basis. Take these steps to insure passersby do not have access to your system.

- ✓ Ask employees to lock their screens when they are away from their desks.
- ✓ Use theft prevention devices for computers and hardware located in easily accessible places.
- ✓ Ask that employees orient workstations to ensure their screens are not visible to others.
- ✓ Require computers to be shut down in the evening.

Use the Microcomputing Security and Duckware CD - Ask for a copy of the Microcomputing Security and Duckware CD for your department's use. This CD automatically configures your machine to enable a number of critical security settings. It available at the Microcomputer Services Helpdesk in 151 McKenzie Hall, or call them at (541) 346-4412 and request a copy via campus mail. If you have technical support available at your location, confirm with them before installing this product.

Keep your System Updated

- In cooperation with your technical support, institute an automatic update policy. Systems that are not kept up to date are susceptible to attack.

Use Safe Browsing Practices – Most of us complete Internet research associated with our positions. Usually, our computers have a default browser on them such as older versions Internet Explorer which can be susceptible to viruses.

- Use a safe internet browser for general browsing such as Mozilla Firefox or Internet Explorer 7 instead. You can download Mozilla Firefox at http://www.mozilla.com or Internet Explorer 7 at http://www.microsoft.com/windows/ie/default.mspx.
- Do not visit suspicious or unfamiliar websites. If you must visit them, do not type any personal information into them.

Avoid Spam - All of us receive plenty of spam and unfortunately, some of us are forced to allow emails into our computer from unknown sources because of our positions.

- If you receive an email that you're not sure of, check with your technical support staff before opening it. If you don't have support staff, call (541) 346-4412 for assistance.
- You can reduce the amount of spam you receive by checking your spam filtering settings. You can do this at http://password.uoregon.edu/spam/. There is additional information available on configuring your spam settings at http://micro.uoregon.edu/email/junk/index.html.

Sensitive Information – Be sure your staff knows which information is sensitive and could be detrimental if distributed to the wrong parties. Stress the importance of following standard security practices to protect this information, proper use of this information and repercussions should the information be disseminated.

- Do not save sensitive data to your computer unless it is absolutely necessary you do so.
- Talk to your technical support staff about ways to insure safety of sensitive information on your network.

Useful Contact Information

Acceptable Use
http://cc.uoregon.edu/policy/acceptable_use.html
abuse@uoregon.edu
(541) 346-1635

Microcomputer Services Help Desk
http://micro.uoregon.edu/
microhelp@lists.uoregon.edu
(541) 346-4412

Security Incidents
http://security.uoregon.edu
security@uoregon.edu