

Quick Reference Guide

Additional Resources

Students:	SCS HelpDesk	509-335-4357	helpdesk@wsu.edu
Faculty, Staff & Affiliates:			
	• <i>Computer & Telephone Accounts</i>		
	IT PhoneDesk	509-335-3663	phonedesk@wsu.edu
	• <i>Technical Assistance</i>		
	Technical Assistance Center (TAC)	509-335-5396	tac@wsu.edu
	• <i>Contact your local system administrator</i>		
WSU Spokane:	HelpDesk Center	509-358-7748	spok.it.help@wsu.edu
WSU Tri-Cities:	Computer Center HelpDesk	509-372-7334	tchelp@tricity.wsu.edu
WSU Vancouver:	Information Services	360-546-9770	wsuvhelp@vancouver.wsu.edu
ICN (Spokane):	IT HelpDesk	509-324-7311	icnhelp@wsu.edu
Barracuda Spam Filtering	-----		http://www.wsu.edu/nospam
University Advisory Committee for Computing & Telecommunications	-----		http://www.wsu.edu/uacct
WSU Copyright Office	-----		http://publishing.wsu.edu/copyright/
Cougar Technology Orientation	-----		http://www.wsu.edu/cto
Symantec Antivirus Implementation Procedures	-----		http://www.wsu.edu/navce
Operating Systems Update Sites			
	• <i>Microsoft</i>	http://windowsupdate.microsoft.com/	
	• <i>Apple</i>	http://www.apple.com/support/downloads/	
	• <i>Linux</i>	http://distrowatch.com/	
WSU Policies and Procedures			
		http://www.wsu.edu/policies.html	
		http://www.wsu.edu/~forms/manuals.html	

Campus Police	509-335-8548
http://www.wsu.edu/police	police@wsu.edu
ITS Security Group	509-335-3900
http://www.wsu.edu/itsecurity	abuse@wsu.edu



Six Basic Security Steps

Secure your area

- Secure equipment and data before leaving an area unattended
- Physically lock down laptops and workstations whenever possible
- Close down your browser after visiting a web site with sensitive data
- Log off or enable a password protected screen saver when you step away
- Do not leave sensitive papers or data on printers or fax machines

Secure your computer

- Enable the operating system firewall before you connect to the internet*
- Disable automatic login and guest accounts*
- Do not install or open unknown programs or files
- Do not share directories or files with others
- Password-protect your screen saver and set it to start after fifteen minutes of inactivity

Keep up-to-date

- Check frequently for updates for:
 - Operating System
 - Browser
 - Application Software
 - Antivirus Client and Definitions
- Turn on Automatic Updates*

Set strong passwords

- Construct good passwords with:
 - A minimum 8 characters
 - A combination of upper and lowercase letters, digits and special characters
- Protect your password
 - Do not reveal your password to others
 - Do not write down or post your password

Protect your computer from viruses

- Use WSU provided Symantec Anti-Virus software
- Use antivirus software on home computer
- Ensure your virus definitions are current
- Turn on Auto-scanning and Real-time protection*
- Scan all removable media and email attachments

Backup your data

- Backup important data to removable media or an appropriate backup service
- Backup frequency and method depend on data's value
- Secure backup media to protect sensitive data

*See <http://www.wsu.edu/itsecurity> for instructions on how to modify these settings.

*[http:// www.wsu.edu/itsecurity](http://www.wsu.edu/itsecurity)
The IT Security website has help
and documentation on the following topics*

Common Security Risks

Storing University non-public or confidential data on your workstation or laptop without proper security precautions.

Identity Theft

The Federal Trade Commission (FTC) states that identity theft has reached epidemic proportions and is the fastest growing crime today. It is imperative that we properly protect any personal or financial information that we maintain or process that could be used for the purpose of identity theft.

Prevent Identity Theft

- Give personal information only when necessary.
- Beware of unknown callers or email.
- Guard confidential data.
- Use only secure e-commerce sites.
- Encrypt email containing sensitive information.
- Ask your supervisor if you are unsure.

Social Engineering

Social engineering is an attempt to trick a person into revealing sensitive information or confidential data. Social engineering uses email, web sites, phone communication and other means to gather data.

- Don't become an unwitting accomplice by being too trusting or eager to help.
- Guard others' private or confidential information, just as you would want others to guard yours.
- Ask who has authorized this request so that you may verify the authorization. If you are not authorized to provide that information, offer to help locate the correct person.
- Ask your supervisor if you are unsure.

Phishing and Pharming

Phishing and pharming are automated social engineering techniques used to obtain confidential information under false pretenses, often through the web or email, for example an official-looking email asking you to verify or update your credit card information with a link to a look-alike web site.

Spyware

- Beware of "free" software, peer-to-peer file sharing, and unknown websites. Software that can monitor and control your computer use, steal your passwords and data could be installed without your knowledge.
- Periodically use spyware detection and removal tools.

Spam Email

- Do not reply to spam or suspicious email.
- Set your email client to prevent automatically opening email or attachments.
- Delete Spam messages and attachments before they are opened.



Creating a Network ID (NID):

Creating your network ID is a simple process. To get started, go to <http://www.wsu.edu/NID>
You will need to have your WSU number and personal information.



Resetting a Network ID Password:

To reset a forgotten password, go to <http://www.wsu.edu/NID>
You will need your Network ID, your WSU number and your birthdate.



Resetting other WSU Passwords:

To reset other WSU passwords contact the WSU PhoneDesk or your system administrator.

Laws, Policies & Procedures

Federal Laws:

- FERPA – Family Educational Rights and Privacy Act (1974)*
- DMCA - The Digital Millennium Copyright Act (1998)*
- GLBA – Gramm-Leach-Bliley Act (1999)*
- HIPAA – Health Insurance Portability and Accountability Act (2000)*

Washington State - Revised Code of Washington (RCW):

- RCW 42.52 -Ethics in public service*
- RCW 42.52.160 Use of persons, money, or property for private gain*
- RCW 42.52.180 Use of public resources for political campaigns*

Washington State - Washington Administrative Code (WAC):

- WAC 292-110-010 Use of state resources*

Washington State University Executive Policy Manual:

- Electronic Publishing Policy – EP4*
- University Data Policies – EP8*
- Wireless LAN Policy – EP13*
- University Antivirus Policy – EP14*
- University Network Policies – EP16*
- Computer and Network User Identification and Password Policy– EP18*
- University Domain Name Policy – EP21*
- University Electronic Correspondence Policy – EP23*