Secure and Safe Computing Primer

Examples of Desktop and Laptop standards and guidelines

1. *Implement anti-virus software*

An anti-virus program is necessary to protect your computer from malicious programs, such as: virus, trojan, worm, etc. Implement credible and reputable anti-virus software and keep it up-to-date.
Note that an anti-virus application cannot stop viruses that it does not know about. Therefore, it is very important to keep the definition database up-to-date by configuring automatic update of the definition list daily; but be sure not to set it to a time when the machine will be turned off.
Enable the real-time protection functionality and perform regularly scheduled full system scans because these features will identify, stop, and quarantine a virus as it attempts to execute.

2. Implement anti-spyware

Malicious software created with the intention of financial gain (e.g., with the creator being paid for every advertisement he can pop up on your desktop, going to market with your private information, or even assuming your identity to make purchases, etc.) is referred to as spyware.
Spyware is often installed on your machine via tagging along with a game or application that you want to use, or it can be installed by certain network worms. Once it is in your computer, it then begins collecting information about you and your activity, and then it sends the information to someone else.
Install an anti-spyware program, and keep the definition database up-to-date via configuring automatic update of the definition list daily; but be sure not to set it to a time when the machine will be turned off.

3. Enable the built-in firewall and/or use a third party firewall program

A firewall program is an application that limits the types of connections that the rest of the world can make to your machine. Major operating systems have a built-in firewall that is simple to implement and does not interfere with your normal use.

If you are connected to a network or the internet, install a firewall application, some are available for free, which will offer you more robust protection than the operating system's built-in firewall.

4. Regularly check for and apply vendor security updates for your operating system and applications

Operating systems are made up of numerous components with different functions and some of these components are vulnerable to exploits. Hackers are continually probing and testing for vulnerabilities in all the major computer operating systems and are generally pretty adept at finding them. When this happens, the company that markets and distributes the operating system rushes to develop a patch to fix the problem and makes it available at no charge to users of the operating system. The problem is many users rarely check for availability of patches and system upgrades and apply them. Major operating system vendors offer mechanisms that will allow you to regularly check for updates and apply them relatively easy.
A service pack is a collection of the critical updates and often includes major updates to the operating system. Some updates cannot be loaded until the latest service pack is installed. Periodically ensure that you are on the current service pack.
Likewise, there's often a security aspect to individual software applications (word processing, spreadsheet, database, etc.) as well.
When system and application updates are available, implement the security updates.

5. Implement a strong password syntax and protect your password

The key for complete access to your computer is your password. There are countless programs that attempt to determine passwords, both by guessing common ones and by randomly generating possibilities and trying them all, or a combination of the two. The best defense is a strong password. This makes the password nearly impossible to guess in a reasonable amount of time.
A strong password is at least 8 characters long, has a mixture of at least three of the following: UPPERCASE (A-Z), lowercase (a-z), digits (0-9), special characters (@#$%&*, etc.). Avoid whole dictionary words and names or phrases that people with personal knowledge of you might be able to guess. The longer the password, the harder it is to guess.
Always use strong passwords. Change your password if you think it has been compromised.

Don't share your password with anyone, and don't write it down. If you must write down passwords, keep the information secured and do not write down the corresponding ID.

6. *Logout of finished sessions and lock computer when left unattended*

All major operating systems provide the ability to "lock" and password-protect the screen and system so that an unauthorized person with physical access cannot tamper with your computer.
Every time you leave your computer, logout the session if you no longer need access to the system and/or enable password-protected screensaver to lock your computer.

7. Physically secure your machine

Never assume any location is completely secured, even if the location is restricted via swipe-access or locked door. There is almost always a way for someone to get to a restricted area.
Never leave an unsecured laptop computer unattended.

8. Protect confidential and sensitive information

Use encryption software to protect confidential and sensitive information/data stored in your computer.
Never send confidential and/or sensitive information via email. If you must send such information via email, encrypt the information before sending it.
USB thumb drives and external hard drives are commonly used to store information and data because of their portability factor. Also note that other mobile devices (e.g., memory cards, iPods, multimedia players, PDAs, etc.) have the capability to store data as well. **If you use portable devices to store confidential and sensitive data, keep them physically secured and encrypt the confidential and sensitive information and data on them** for protection against unauthorized disclosure, as well as, in the event of theft or lost of the device.

9. Scan email attachments before opening them

An effective method by which viruses, trojans, worms and backdoor programs are propagated is via e-mail attachments. If you receive an attachment that you weren't expecting or from someone you don't know, chances are that the attachment carries some variety of malware (malicious software) just waiting for you to set it loose by opening it.
When you get an email attachment, unless you feel very confident about what it is, where it came from, and why it was sent to you - **DON'T OPEN IT!**
Take precautionary measures and scan all email attached files with your anti-virus software even from people you know because their machine could have been compromised and used to propagate the spread of malware.
Be cautious about clicking on links sent to you in email - it is very easy to create a link that hides the true location of where the link goes. You should always either cut and paste the link into your browser, or manually retype it.

10. Refrain from using the save password features for sensitive applications

Various programs (e.g., email programs, web browsers, etc.) can be configured to save user name and password information. This can be convenient for you, but if you share your computer with others, they will also have access to your accounts. Additionally, if your computer is lost or stolen, then the saved account passwords are now compromised.

Turn off password save features.

11. Disable unused accounts

Some operating systems have predefined user accounts (e.g., 'Guest' account, etc) that are well known and commonly exploited because the user doesn't always change their default settings, including the default password. To protect your computer, the unused accounts must be disabled and/or deleted to prevent anyone from using them to login to your computer.

If you need to keep a default account, ALWAYS change the default password.

12. Disable all unused services

All major operating systems come packaged with all sorts of application and server software. These services include: ftp, telnet, SQL, SMTP (e-mail server), Apache (web server) and others. Vendors often turn these services on by default and frequently give you very little explanation about what they do and little flexibility with regard to configuration settings. In general, the more services you have running on your computer, the more potential targets you have for hackers to exploit, not to mention slowing down your computer running things you don't need. When considering what services should be running on your system, here's a simple rule of thumb:

- **If you don't know what it is or what it does, *don't turn it on.* In most every case, if you find out later that you need it, you can go back and turn it on.**
- **If it's on, and you don't need it, *turn it off.***
- **If it's off, and you don't need it, *don't turn it on.***

13. Create regular backups

There is the potential that files may be lost or corrupted due to hardware and/or software failures, and/or human errors (e.g., unintentionally deleting the file), and having another copy of your files prior to such catastrophe will alleviate the burden of recreating the lost or corrupted files to their original form.

There are numerous software solutions that will back up everything on your machine. An effective and low cost backup alternative is simply copying the files/data on a CD and keeping it in a safe and secured location.

Perform regularly scheduled (e.g., daily and/or weekly) backup of your files/data.

The backup frequency should be based on the importance of the data and the frequency of change to the data. If you use backup software, the software will typically provide you with the option to schedule the backup on a regular basis. Alternatively, if you manually create backups to CDs, perform the task on a regular cycle.

If your backups contain confidential and/or sensitive files/data, ensure that you have provided the same level of security protection (e.g., encryption) as you would for the original files/data.

14. Be alert and aware of information stealing techniques

Social engineering is a collection of techniques used to manipulate people into performing actions or divulging confidential and sensitive information, such as password, social security number, etc.
A technique in phishing scams is using either email or regular mail to obtain personal and sensitive information from you. For example, a common phishing scam is an email informing you as the winner of a 'lottery' but to collect you must supply them your banking information to initiate the transfer of funds. Another recent phishing scam is an official looking email from your bank or financial agency stating there is a problem with your account and telling you to verify your credentials via a weblink in the email or your account will be deactivated. If you click on the weblink, the website may appear to look official, some sites even forged the company's logo to make it appear legitimate, but the site is setup to steal your personal and sensitive information.
If you receive emails from your bank or financial agency, always verify with the agency by contacting them directly (e.g., calling customer service) and explain to them the situation and that you would like to verify its authenticity.
Especially when using your computer in open or public areas, be alert to shoulder surfers – people who look over your shoulder while you type in your user name and password or other sensitive information.

15. Sanitize your computer before donating and/or disposal

Before selling, donating, or discarding old computers, make sure that sensitive data is removed. Files that are simply deleted can be easily recovered. To sanitize your hard drives, use a program designed to overwrite the drive in a secure manner, formatting your drive does not remove the data effectively. See your system administrator for more information on acquiring a copy of the software to sanitize your hard drives.