COLUMBIA UNIVERSITY
INFORMATION TECHNOLOGY

Workstation Security Best Practices - User Guide

1. Check for vendor security updates and apply them. Periodically, security weaknesses in the operating system and/or application are discovered and the vendor will then provide security updates to remediate such security exposures. Enable the automated feature in major operating systems (i.e., Windows and Macs) that checks for security updates. When notified of the security updates availability, review the update and then apply update as appropriate.
2. Enable the built-in firewall that is included in major operating systems (i.e., Windows and Macs). A firewall is an application to restrict others from connecting to your computer. The firewall application should be set to restrict access unless required by specific applications.
3. Implement credible and reputable anti-virus software (e.g., Symantec Antivirus), perform continuous and/or scheduled scanning, and keep it up-to-date. An anti-virus program will protect your computer from malicious programs. The software must be operating at all times in real-time scan mode, the virus definition list shall be updated at least once a day, and schedule a full system scan weekly.
4. Implement anti-spyware to protect your private information. Spyware is a class of programs designed to steal personal information. The software must be operating at all times and the definition list should be maintained up-to-date.
5. Establish strong password syntax (i.e. 6 or more characters in length (8 or more characters in length is preferred), mix of alphanumeric and special characters) and protect your password. A password is used to provide authentication to an application and/or system. Never share your password with anyone even family members.
6. Limit your computer usage to yourself and restrict others from using it especially for internet access because they may unintentionally download malicious software (e.g., key logging program).
7. Do not copy or reproduce any confidential and/or sensitive information/data, except as required in your official job capacity.
8. Confidential data should not be transferred offsite (e.g. home) using email, file dropboxes, portable storage devices, etc. unless encrypted and specifically authorized.
9. Do not store any confidential and/or sensitive information / data on your desktop, laptop or on any media, except as required in your official job capacity
10. If you need to store any confidential and/or sensitive information / data on your desktop, laptop or on any portable media devices, you must implement the appropriate security controls to protect confidential and sensitive information / data as established by the Columbia University's Data Classification and Encryption policies (i.e., http://policylibrary.columbia.edu/data-classification-policy and http://policylibrary.columbia.edu/encryption-policy)

    Also refer to Columbia University's most current specification of workstation security requirements as specified in the document "Desktop/Laptop Security Requirements" (http://policylibrary.columbia.edu/desktop-and-laptop-security-policy). These documents describe additional security requirements such as the need for encryption.

Note: For items 1, 2, 3, 4, 5, and 10

If you are using a Columbia University issued/managed computer, then enforcing the above controls is the responsibility of your IT support department.

If you are using a computer other than a Columbia University issued/managed computer, then you are responsible for enforcing the above controls.

Implementation of additional controls are required for workstations that access or store sensitive information such as no local administrative user privileges, password-protected screen saver, desktop management agent, encryption of local hard drive, other storage devices, and sensitive email attachments, no peer-to-peer software, and secure remote access.