13.1.2 Workstation Security Facts

When managing workstations, there are several key security best practices that you should be aware of:

Practice	Description

Implement the Principle Of Least Privilege	Users should have only the degree of access to the workstation necessary for them to complete their work and no more. Observe the following:
	▪ Only those users who need administrative access should have it. You should use limited user accounts for everyone else. Don't make a user a member of the Administrators group unless the user needs administrative access to the system.
	▪ The workstation should have the software required for it to fulfill its function on the network and no more.
	▪ Use delegated administration. Don't make all admin users members of the Administrators group. Make admins members of the Windows group that most closely matches the level of access they need:
	  ▪ Backup operators: members of this group can backup or restore files, regardless of permissions assigned to those files.
	  ▪ Cryptographic operators: members of this group can perform cryptographic operations.
	  ▪ Network Configuration Operators: members of this group can manage the IP configuration on the system.
	  ▪ Performance Log Users: members of this group can manage performance logs and alerts.
	  ▪ Performance Monitor Users: members of this group can manage performance counters.
	  ▪ Remote Desktop Users: members of this group can remotely access a workstation's desktop.

Require Passwords	All user accounts should have a password assigned. Passwords should also be required to unlock the screensaver and to resume from standby or hibernation.
Use Strong Passwords	A strong password is one that: ▪ Is at least 8 characters long (longer is better) ▪ Is not based on a word found in a dictionary ▪ Contains both upper-case and lower-case characters ▪ Contains numbers ▪ Does not contain words that can be associated with you personally ▪ Is changed frequently
Use File and Folder Permissions	This practice ties back to principle of least privilege. Users should be able to access the files and folders they need on the hard drive of the system and no more. Use file and folder permissions to explicitly specify who can do what with files and folders.
Disable the Guest User Account	The Guest user account has no password and provides too much access to the system. The Guest user account should remain disabled.
Don't Use Default User Names	Avoid using default user names, such as Administrator. Change these names to something else.
Disable Autorun	Disable autorun. This prevents malware from automatically running when an optical disc or USB drive is inserted in the system.
Install Privacy Filters	A privacy filter is a polarized sheet of plastic that is placed over a computer screen to restrict screen visibility from any angle other than straight on. This prevents office guests and passers-by from being able to read information from the user's computer monitor.
Block Untrusted Software Sources	Software from untrusted sources could potentially contain malware. In fact, many modern network exploits attempt to trick users within an organization into downloading and installing malicious software. By doing this, an attacker can easily circumvent network security devices and launch an attack from behind the firewall. To prevent this from happening, consider the following:

- Restrict user's ability to install software. For example, standard users on a Windows system are not allowed to install any software.
- For users that are allowed to install software, restrict them to trusted software sources. For example:
  - Software for desktops and notebooks should be restricted to trusted software publishers, such as Microsoft or Adobe.
  - Software for mobile devices should be restricted to trusted app stores such as Google Play, the Microsoft Store, or Apple App Store.
- No user should be allowed to download and install software from untrusted sites on the internet. Unknown software publishers should be carefully investigated before allowing their software into your organization.