13.3.7 Physical Security Facts

Data loss prevention (DLP) is a strategy for making sure that sensitive or critical information does not leave the corporate network. Compliance policy should be implemented to regulate company rules and expectations. This should be clearly communicated to the employees. By enforcing compliance policies, the organization will be safeguarded against any laws and government regulations that employees may break.

Be aware of the following methods for protecting computers:

<table>
<tr><th>Method</th><th>Description</th></tr>
<tr><td>Building Security</td><td>The first line of defense in protecting computer systems is to control access to the location where the computers are located.
<ul>
<li>Many businesses use cubicles which leave computers in plain sight and easily accessible to anyone. Controlling access to the building is critical to prevent unauthorized people from gaining access to computers.</li>
<li>Place critical or sensitive devices in a locked room.</li>
<li>Move printers used for confidential documents away from public areas.</li>
<li>Disable network jacks in public areas, such as reception areas.</li>
</ul>
For good physical security, implement the following protections:
<ul>
<li>Implement controlled access to any point inside the building beyond the lobby (such as locking doors and security checkpoints).</li>
<li>Require all authorized personnel to have identification while inside the building.</li>
<li>Escort visitors at all times.</li>
<li>Keep room doors locked when not in use.</li>
<li>For added protection, use keypads or card readers to control building or room access.</li>
<li>Use software to track who has gained access at any given time.</li>
<li>Periodically change passwords or locks, especially after key employees are terminated.</li>
<li>Implement mantraps. A mantrap is a specialized entrance with two doors that creates a security buffer zone between two areas.
<ul>
<li>When a person enters into the space between the doors, both doors are locked.</li>
<li>To enter the facility, authentication must be provided. This may include visual identification and identification credentials.</li>
<li>Mantraps should permit only a single person to enter and authentication must be provided by each person.</li>
<li>If authentication is not provided, the intruder is kept in the mantrap until authorities arrive.</li>
</ul></li>
<li>Security guards can use an <i>access list</i> (sometimes called an <i>entry control roster</i>) which explicitly lists who can enter a secure facility.</li>
</ul></td></tr>
<tr><td>Hardware Locks</td><td>Hardware locks prevent theft of computers or components.
<ul>
<li>Keep servers and other devices inside locked cabinets or locked rooms.</li>
<li>Bolt or chain workstations to desks or other stationary objects to prevent theft.</li>
<li>Lock cases to prevent opening up devices and removing components such as memory and hard drives.</li>
<li>For laptops, use removable cable locks when leaving computers unattended in public areas (such as a library). You can also use motion detectors that sound an alarm when a laptop is moved.</li>
<li>Tablet devices can be secured with a cable lock or simply locked in a cabinet or drawer when not in use.</li>
</ul></td></tr>
<tr><td>Lock the Workstation</td><td>You can set the following passwords in the BIOS to require a password when booting or when modifying BIOS settings:
<ul>
<li>Configure a user password to require the password before loading the operating system.</li>
<li>Configure an administrator password to require the password to edit BIOS settings.</li>
<li>Configure a hard disk password to require the password before data on the disk can be accessed.</li>
</ul>
Leaving your computer unattended while you are logged on potentially gives free access to your computer. Use the following methods in Windows to secure unattended computers:
<ul>
<li>Configure the screen saver to display the logon screen. The screen saver will be activated automatically when the system is inactive for a period of time.</li>
<li>Press the <b>Windows logo</b> key + <b>L</b> to lock the workstation.</li>
</ul></td></tr>
</table>

	▪ Under Personalization in Control Panel, require a password when the computer wakes up. When leaving the computer for an extended time, use the keyboard sleep button to put the computer to sleep.
Computer Tracking Service	If you are concerned about stolen devices being used to view confidential data, you can sign up for a computer tracking service. These services can help locate stolen devices, or take other actions such as deleting data or disabling the device. Remember that: ▪ Most services use the IP address or a wireless signal to locate the device. The device must connect to the internet to be located. ▪ Tracking protections might work only as long as the original hard drive has not been reformatted. ▪ Some device manufacturers can help you track stolen devices by registering the service tag on the device. If technical support is requested for a stolen device, they can alert the authorities. ▪ Many mobile devices can be remotely disabled using cellular signals that do not rely on an internet connection.
Removable Storage	Removable media is any type of storage device that can store data and be easily removed and transported to other locations. Removable media includes floppy disc, tape, USB/flash storage, CD/DVD, and external hard drive. Removable storage: ▪ Increases the threat of removal and theft of sensitive data. Users can copy sensitive data to portable devices, or media containing data may be lost or easily stolen. ▪ Increases the chances of introduction of malware. Be aware of the following recommendations for protecting removable media: ▪ In secure environments, remove and disable removable media devices to prevent copying data to or from the device. You can disable USB and IEEE 1394 ports in the BIOS and require a BIOS password to edit BIOS settings. However, this may also disable necessary USB devices such as the mouse and keyboard. You can use endpoint management software to disable USB ports on a system if storage devices are connected, but enable them if a mouse or keyboard is connected. ▪ Use USB port locks to block all ports and ensure no USB will be inserted into the devices. ▪ Keep backup media and other removable media in a secure location. ▪ If possible, use disk encryption to prevent users from being able to read data on removable media.
Storage Media Disposal	When disposing of data storage media, make sure to remove any sensitive data, especially data containing personal health or financial information. Simply deleting data is insufficient as deleted files can still be recovered. *Data remanence* are remnants of data (after the data has been erased) that allow the data to be recovered and reconstructed by data recovery software. ▪ If you will be reusing a disk, use data wiping software to remove any remnants. This software writes a random series of bits multiple times to each cluster on the disk. ▪ When disposing of magnetic media, you can use degaussing with a strong magnet to remove any traces of data. ▪ When disposing of optical media, shred or physically destroy discs (some paper shredders can also handle optical discs). Degaussing does not work with optical media because the media does not use magnetic fields for storing data.
Mobile Devices	Some organizations implement security policies that forbid users from connecting their personal mobile devices to the organizational network (wired or wireless). Some organizations allow mobile devices; in fact, they may even provision users with mobile devices. However, there is a risk in this situation that company data may be copied to these devices that could be compromised if a device is lost. As a safeguard, many of these organizations require that remote wipe be enabled on the device such that if it is lost or stolen, a command can be sent remotely to the device to remove all data on it.