4.2.3 Hardware Security Facts

Physical security of computers is important because it is relatively easy to bypass security passwords with software utilities. Physical security for hardware should be based on the requirements of each site. Be aware of the following general hardware security guidelines:

Guideline	Description
Checkout Policy	A checkout policy ensures that hardware does not leave the organization's premises without a manager's approval. Checkout policies could include the following details: ▪ Acceptable use is limited to business-specific activities on the device. ▪ Software that is included on the device. ▪ Identifying characteristics of the hardware such as the serial number, make, and model number. ▪ A rule that borrowers must not install software on the devices. ▪ A rule that returning the device should be within a reasonable or defined period. ▪ A rule that liability is placed on the borrower for the device's physical safety and damage.
Room Security	The first line of defense in protecting computer systems is to control access to the location where the computers are located. ▪ 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. ▪ Place critical or sensitive devices in a locked room. For good physical security, implement the following protections: ▪ Keep room doors locked when not in use. ▪ Use keypads or card readers to control room access. ▪ Do not leave the door ajar due to high temperatures.
Hardware Locks	Hardware locks prevent the theft of computers or components. ▪ Keep servers and other devices inside locked cabinets or locked rooms. ▪ Bolt or chain workstations to desks or other stationary objects to prevent theft. ▪ Lock cases to prevent opening up devices and removing components, such as memory and hard drives. ▪ For laptops, use removable cable locks when leaving computers unattended in public areas. You can also use motion detectors that sound an alarm when a laptop is moved.
Backup Storage	A *backup* is a copy of data that is archived and can be used to restore data. ▪ Backup media should be stored in a secure location. ▪ Keep backup media in a locked cabinet or safe (preferred).