

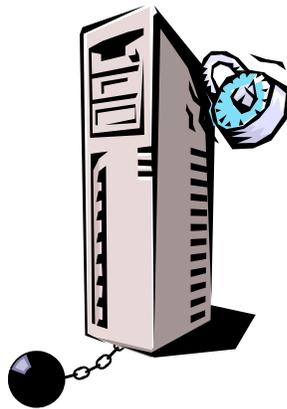


4.6 SAFEGUARD ASSETS: SECURE COMPUTERS AND NETWORK EQUIPMENT

Network servers, user workstations, portable laptops, wireless devices, and other equipment such as printers, modems, and the like should be secured to avert losses. Whether by water damage, theft, or unauthorized access, computer equipment is vulnerable to misuse or physical damage. Here are a few protection techniques to physically safeguard user workstations, portable laptops, PDAs, wireless devices, and other equipment:



A. PC Workstations



1. Bolt down equipment. Whether in the office or at home, secure computer equipment to workstation furniture so it cannot be removed easily. Purchase relatively inexpensive PC security kits to anchor PCs to furniture or other equipment. For example, the Kensington MicroSaver cable locking system uses pry-resistant security plates that bond (glue) to PC equipment and bond (glue or screw) to your desk. Other kits use systems such as locking bracket kits that mount to any vacant expansion slot on the PC. While this technique may not be cost-effective on a company-wide basis, it is effective for equipment in high-traffic areas or unattended, as well as portable/laptop computers while parked in the office.

2. Install CPU case locks. Prevent people from opening up CPU cases to steal CPU microprocessors, hard drives, RAM memory chips, video chips, monitor cards, and other components with a CPU case lock, also called as universal cabinet lock.

3. Use disk drive locks. Use disk drive locks to prevent unauthorized access to information on computers. Disk drive locks slide over the floppy disk drive or CD-R or DVD-R drive bay to prevent others from copying data or introducing a potentially harmful virus. This type of device is ideal for portable PCs since the disk drive lock can be used with a cable that can loop around a desk or table leg to secure the entire system.

4. Purchase diskless workstations. Use diskless PCs for selected workstations to prevent the downloading of files or data.

5. Use a CPU stand/keep off ground. Reduce the risk of the CPU's being bumped and other accidents by placing it in a CPU stand under a desk or work counter. These stands usually come in plastic or metal and hold the CPU in a space-saving vertical position. However, avoid carpeted areas where CPUs risk hard disk data loss from static electricity and powerful vacuum cleaner magnetic motors. Keep CPUs off the ground to prevent water damage from sprinklers or plumbing leaks.

6. Install static-release pads. Prevent static electricity from burning out a computer's circuitry with static-release pads. These plastic mats sit under workstation chairs or keyboards and have a wire connected to a wall outlet ground screw. Touching the mat releases damaging static.



4.6 SAFEGUARD ASSETS: SECURE COMPUTERS AND NETWORK EQUIPMENT

(CONTINUED)

B. Portable Computers, PDAs, and Other Wireless Devices



- 1. Use a padded carrying case or compartment for travel.** Protect portable computers by using padded carrying cases with a separate secure compartment.
- 2. Use antitheft protection/lock it down.** Tie down laptops to furniture whenever you are traveling by using a cable locking system like the Kensington security cable, which uses the security slot (a small hole with a chain logo above it on the frame of the laptop).
- 3. Use alarms and antitampering devices.** Use movement and distance sensors like DefCon that will set off an alarm if the laptop is moved. These systems can detect unauthorized tampering and even make data unusable if proper authentication has failed.
- 4. Require “credit card” token to access laptops.** Use credit card-sized tokens to lock and unlock the screen.
- 5. Encrypt data on laptops, PDAs, and other wireless devices.** Encrypt valuable data on the laptop hard drives to limit access and to make stolen devices useless. Require passwords and tokens to decrypt. (See sections 5.10–5.12.)
- 6. Limit the information kept on portables.** Do not keep valuable data directly on mobile devices. Instead, turn your portable devices into access machines. After inserting a token, generating a dynamic password, and using a secure firewall/VPN connection, log into your company website or network to get data.
- 7. Back up data regularly.** If you do carry valuable information on your laptop, make sure it is periodically backed up.
- 8. Bring laptops in for periodic maintenance and update.** All portable equipment checked out to employees should be brought back in on a periodic basis for scheduled maintenance.

C. All Computer Equipment



1. Cover equipment. When equipment is not in use, use plastic covers to protect it from dirt, dust, spills, and water damage (from fire sprinklers or broken pipes). When placed over keyboards, monitors, and printers, plastic covers (also called dust covers) can extend equipment life and prevent mysterious malfunctions. For continuous protection, cover keyboards with a thin plastic membrane that fits over the keys.

2. Prohibit eating (and drinking) near computers. Make it a company policy that eating near computers is prohibited. Food particles that have fallen into a keyboard can render it useless, and coffee or soft drinks spilled into a computer’s case can destroy it.



4.6 SAFEGUARD ASSETS: SECURE COMPUTERS AND NETWORK EQUIPMENT (CONTINUED)

D. File, Web, and Application Servers and Network Connections



Foremost in the physical security of computer systems is the protection of servers and key network connections. Pay special attention to the location of servers, tape backup units, and network connections such as hubs, routers, switches, and gateway machines, as applicable. Remove physical hazards that may jeopardize the safety of this essential equipment. Without proper protection, network equipment is vulnerable to damage caused by extreme temperature fluctuations, dust, water, fire, power irregularities, and accidental or intentional destructive human acts. Follow these techniques to safeguard servers and other mission-critical network equipment:

1. Keep network server(s) and vital connections in a locked room with access limited. If possible, dedicate a special room or office in the interior of the building (without windows) as the network data center. Ideally this room should be installed with raised flooring, cable trays, and prewired cabling, as well as dedicated power, cooling, and fire suppression systems, as described below.

2. Attach separate backup power to network equipment. Avoid abrupt power loss and potential loss of data or equipment damage with a power protection device such as a UPS. Keep mission-critical computers running with a backup power generator. (See section 4.10.)



3. Maintain a temperature-controlled environment. Provide climate control, air conditioning, and regulate room temperature to prevent damage from temperature fluctuations due to network equipment heat buildup. Do not forget to attach backup power generators to cooling systems as well.

4. Install fire prevention equipment. Equip computer rooms with special fire suppression systems such as sprinklers, Halon, or more environmentally friendly dry standpipe systems. Keep handheld portable fire extinguishers nearby to stop small fires before they become big ones.



5. Raise servers off the ground. Raise file servers and other network equipment at least two inches off the floor to protect it from water damage (e.g., if the sprinklers go off in the building or flooding occurs from bathroom/kitchen plumbing failure).

6. Use special racks to hold network equipment. Install protective enclosures to shield network equipment from falling objects. Also secure equipment so that it does not tip over or get bumped. Purchase prefabricated computer shelving units or equipment racks specially designed to secure and organize various network computers and equipment.

7. Avoid damage from static. Protect network equipment from damaging static electricity by removing carpet and/or adding antistatic floor mats.

8. Use keyboard locks. When they're not in use, disable server keyboards to eliminate possible misuse by setting the keyboard lockout at the console.