

PHYSICAL SECURITY

4.1 General. Physical security deals with the physical actions and measures taken to protect the Service's automated information systems, their components, and operators of those systems. Every location is different and requires an evaluation tailored to its unique circumstances. The following covers some of the more common topics and is provided for use in reviewing local physical security requirements.

4.2 Network and Telecommunications Facility Security

A. All network accessible servers, routers, and telecommunications systems should reside in dedicated locked areas protected by positive access controls. Such areas can be ventilated cabinets or closets for small facilities. Some examples of positive access controls would be key or combination locks, cipher locks, magnetic card scanners, armed guards, or some combination of the items listed.

B. Access to all network accessible servers, routers, and telecommunications systems should be limited to staff (including contractors) directly assigned to work on those systems.

C. The workspace containing these components must be secured when the area is unattended.

D. Whenever possible, these components should be located in areas where access is not possible via raised flooring, removable ceiling panels, or solid walls that do not meet the ceiling.

E. For facilities located on ground floors, additional precautions may need to be exercised. If there are windows, make sure they are locked and where appropriate, reinforced with bars or wire mesh.

4.3 General Workspace Security.

A. Ensure that the workspace containing PCs is secure when the area is unattended.

B. Do not leave small portable computing equipment such as portable computers, laptops, or PDAs exposed. These high value items can be easily removed and account for significant losses each year.

C. We encourage all personnel to challenge strangers in the work area. Under no circumstances should someone unknown be allowed to wander unescorted through work spaces. All personnel who do not reside in the work area, including repairmen and maintenance personnel, should be escorted and under observation at all times.

4.4 Electrical Conditioning. Electrical issues are of major concern in dedicated computer facilities, but there are aspects of the electrical environment that are worthy of consideration by all system users and operators.

- A.** All computing equipment should be connected to the power supply via a surge protector/line conditioning device. These devices help regulate the power supply, which prevents damage to delicate electrical components due to surges or spikes and improves reliability.
- B.** Computing equipment should not be connected to the same power supply as coffee pots, microwaves, fans, or other electronic equipment.
- C.** Computing equipment should not be located in close proximity to electrical transformers, switching devices, telephone switching facilities, power closets, or any other source of magnetic pulse. The currents or pulses from these devices can severely damage magnetic recording and processing media.
- D.** In network and telecommunication facilities, all emergency off switches should be protected from accidental activation.
- E.** All cipher doors and fire alarm systems should be backed up with batteries in case of emergency.
- F.** Power cables and lines should not be in exposed traffic areas where they could be easily tripped over or damaged by foot traffic
- G.** Emergency “negative power” lights should be provided for safety purposes in the event of power loss.

4.5 Fire Protection. Fire is one of the greatest single threats to the users and operators of automated information systems. Every facility must have a fire control and evacuation plan for its personnel.

- A.** Have emergency numbers for fire, police, doctors, and hospitals posted in several publically accessible locations.
- B.** Conduct periodic fire drills. Make sure everyone knows how to operate the fire extinguishers, who to call, where the power switches are, the best exit from the building, etc.
- C.** Ensure that electronic doors will function in a manual mode in case of power failure. Do not block exits.
- D.** Store all combustible supplies in a well ventilated area away from electrical equipment. Paper dust is highly combustible and can be explosive.
- E.** For computer rooms or dedicated processing facilities:
 - (1)** Do not allow smoking in the computer room or close to the supplies.

(2) In areas with raised floors, have smoke alarms located under the floor. Where practical, have smoke detectors installed in air ducts, ceilings, and equipment locations. Have them tested and serviced regularly.

(3) Know the location of emergency power switches and turn power off before departing the area if this can be done without additional personal risk. Ensure the emergency off switch also shuts down the air conditioning, heating, and other electrical components.

(4) Have hand-held extinguishers strategically located around the work area. Try not to use the dry chemical type of extinguisher around computing equipment. It contains corrosive agents that will severely damage the equipment, hard drives, and electronic backup media.

(5) Have emergency “negative power” lighting to ensure safe evacuation, especially if the facility does not have windows or other natural lighting.

(6) Be aware that magnetic tapes and diskettes produce toxic fumes when burned. Concentrations of these fumes are extremely dangerous.

(7) Critical materials (backups, copy of contingency plans, operating system software, etc.) should be stored in a fireproof safe or container rated high enough to protect the contents.

4.6 Water Protection. One of the leading causes of damage to computer equipment is from moisture.

A. Look around the area and be aware of potential water damage sources such as air conditioner condensation, leaky pipes, water sprinkler systems, non-watertight windows and doors, roof leaks, etc.

B. Do not locate computing equipment next to an outside window, especially if the window can be opened.

C. Do not locate computing equipment close to water pipes, water fountains, or other sources of liquid.

D. Keep hanging and potted plants away from the immediate area of the equipment. They often leak, drip, or produce condensation.

E. Store all computing supplies and software in waterproof cabinets.

F. For computer rooms or dedicated processing facilities:

(1) Eliminate all overhead and under-floor steam or water pipes except for fire sprinklers or other necessary fixtures.

(2) In areas with raised floors, make sure water detection devices are installed. Have them tested and serviced regularly. If the facility is below ground, ensure there is adequate drainage. Install a flood control pump or other siphon device as well as a water detection device.

(3) Ensure all electrical outlets are waterproof, especially if under a raised floor.

(4) Ensure all adjacent areas, restrooms, janitor closets, etc., have adequate drainage to prevent overflow to the computer room.

4.7 Housekeeping Considerations. Cleanliness of the work area, especially the computing equipment area, is vital to continued reliable performance.

A. Areas around the equipment should be kept free from dust, dirt, and moisture. Vacuum the surrounding area; do not dust with feather dusters, rags, spray chemicals, etc.

B. Keep food and beverages away from the equipment.

C. Do not allow smoking within the air exchange radius of a piece of computing equipment.

D. Do not use spray wax or other cleaning compounds on any piece of computing equipment. Use of any cleaning compound should be left to professional maintenance personnel. If you need to clean your machine, follow the manufacturer's guidelines.