**5.3.1 Physical Access and Environmental Controls**

* Physical controls aim to protect information system processing facilities through physical mediums, such as locks, fences, closed-circuit TV (CCTV), and devices that are installed to physically restrict access to a facility or hardware.
* Similarly, environmental controls refer to measures taken to protect systems, buildings, and related supporting infrastructure against threats associated with their physical environment.
* The following are four types of power failure: Blackout: Blackout indicates a complete loss of power. Brownout: Severely reduced voltage, which may place strain on electronic equipment or may even lead to permanent damage. Sags, spikes, and surges: Sag is a rapid decrease in voltage level. Spikes and surges are rapid increases in voltage level. These may result in data corruption in the server or the system. Sags, spikes, and surges may be prevented by using properly placed protectors. Surge and spike devices help to protect against high-voltage power bursts.
* The most effective control to protect against the short-term reduction in electrical power is a power line conditioner. A power line conditioner is a device intended to improve the quality of power that is delivered to electrical equipment. It compensates for the peaks and valleys in the power supply. When the electrical supply is low, it provides its own power and maintains a constant voltage.
* Electromagnetic interference (EMI): EMI is generally the result of electrical storms or noisy electrical equipment. EMI may result in system corruption or damage.
* An uninterruptible power supply (UPS) can help to support an organization from interruptions that last from a few seconds to 30 minutes. An alternative power supply medium (such as a power generator) is most effective when there is long-term power unavailability.
* The following are some of the best practices for the maintenance of an alarm control panel: It should be accessible to security personnel at all times. It should be placed in a weatherproof box. It should have electrical power from a dedicated and separate circuit. It should be placed in adherence to local regulations and requirements.
* Similarly, the following are some of the best practices for the maintenance of water and smoke detectors: In the computer room, water detectors should be placed under raised floors and near drain holes. Smoke detectors should be installed above and below the ceiling tiles throughout the facilities and below the raised computer room floor. The location of the water and smoke detector should be highlighted for easy identification and access.
* Responsibility to be assigned to a dedicated employee for remedial action in case of an alarm. A standard operating procedure should be available. The location of these devices is very important and should be placed in such a way to give early warning of a fire. The power supply of these devices should be sufficient. These devices should be tested at regular intervals. Moreover, an emergency evacuation plan should be posted throughout the facility. Electrical wiring should be placed in fire-resistant panels and conduits. This conduit should ideally lie under the fire-resistant raised computer room floor.
* Physical access control: The objective of physical access control is to restrict and control access to premises, buildings, rooms, and data centers. Examples of physical access control include door locks, security guards, access cards, and so on.
* The following are a few common types of door locks.
  1. Bolting door locks These are traditional kinds of locks that require a metal key to open the gate. For these locks, the key should be under strict control and no one should not be allowed to duplicate the key.
  2. Combination door locks (cipher locks) In combination door locks, access is authorized through a numeric keypad or dial. Access numbers should be available only to authorized people. Access numbers should be changed on a frequent basis and should be mandatorily changed whenever an employee with access is transferred or terminated.
  3. Electronic door locks With electronic door locks, access is granted through a magnetic or embedded chip-based plastic card key. These access cards are difficult to duplicate. It is very easy to deactivate the access card in case of termination or when a card is lost. Alarms can also be configured to monitor unauthorized access However, access card issuance and management processes should be carefully controlled.
  4. Biometric door locks Access can be granted through any of the biometric features of the user, such as voice, retina, fingerprint, and hand geometry. Biometric access controls are generally used for critical and sensitive facilities.
  5. Deadman doors Deadman doors are also known as a mantrap or airlock entrance. In these cases, two doors are used and for the second door to open, the first door must be closed and locked. Only one person is permitted in the gap between the first door and the second door. A deadman door reduces the risk of tailgating or piggybacking wherein an unauthorized person follows an authorized person to gain unauthorized entry. Deadman doors are also used in loading and unloading areas where outer doors open to load or unload from a truck and the inner doors cannot be opened to load or unload until the outer doors are closed and locked.
     + Identification badge: Employees are required to have their identification badges (photo IDs) worn and displayed when in the office. For the comfort of tracking, the badge should be of different colors for employees and visitors. Visitors are required to be escorted by a responsible staff member.
     + CCTV camera: Also, CCTV cameras should be placed at strategic locations. Videos and images should be retained for a sufficient period for 3 months for future requirements. For the security of a high-sensitivity workstation, the use of computer workstation locks will prevent the computer from being turned on. It is advisable not to have facilities such as computer rooms with visible or identifiable signs from the outside.
     + Physical security is as important as logical and should not have any scope of a loophole. It is advisable to define and document the roles and responsibilities of the personnel in charge of physical security.