Chapter 15-IFPO-CPO

Access Control

Access Control

- Access control is the control of access to property, services, events, or information.
- A large part of the protection of assets, personnel, and information begins with controlling access to them and the facilities where they exist.
- Access control provides a means to achieve the desired use and control over assets by allowing access to only agreed individuals.
- The function and practice of access control are fundamental to the protection officer in his or her duties.
  - Checkpoint
  - Guard station
  - No one can enter without proper identification / access
  - **No Authorization / No Access**

Access Control

- Current day access control is achieved through a combination of administrative and engineered controls.
- Elements include technical access control systems and security personnel, record keeping, and policy.
- Uniformed security personnel play major roles:
  - Patrols
  - Fixed checkpoints
  - Control room monitoring

  Physical controls include:
  - Alarms
  - Control rooms
  - CCTV systems
  - Authorization permits
  - Barriers / fencing
  - Checkpoints
  - Warning signage: “No Trespassing” “Authorized Personnel Only” etc.

Emergency Access Control

All access control procedures must consider how to implement safe emergency exits. It is essential that physical security systems are harmonized with the safety of people by not interrupting safe egress from the property or site in the event of an emergency.

- Access should be allowed during an emergency situation.
- Policy should outline that it is imperative to the safety of occupants and employees to allow access during an emergency.
- All work should be halted to allow access
- Areas for access:
  - Elevators
  - Parking lots
  - Loading docks

Examples of Access Control

1. An organization MUST have a policy in place that has a clear definition on property access.
2. Processes:
    1. Documentation
    2. Permits
    3. Work authorization
    4. Visitor and employee badges with modern security features such as holograms and watermarks.

Audit and Record Keeping

Audit and record keeping:

- Sign in access logs, registers, muster lists.
- Serves two purposes.
  1. Leaves a record of who has accessed the site.
  2. Leaves a record for emergency responses purposes in event evacuation is required.
- Training must be provided to maintain governance with complete and consistent files.
- Access control records should be archived for retrieval according to policy.
- Access control records should be treated as “confidential.”
- Once the agreed retention period has been reached, they should be destroyed prior to disposal.

Access Authorization

- Organizations require a clear policy for the denial of access to individuals without proper credentials.
- Supervisors should be consulted when dealing with a denial of access situation.
- If left up to the security office, he/she should err on the side of caution, explain the policy and deny access.
- All denials should be documented in a security report.

Applying Physical Security

- Deployment of physical security measures is only done after the completion of a risk analysis, including a cost-benefit analysis.
- Typical physical security access control measures include:
  - Security personnel
  - Doors, lock, barriers, video systems, alarms
- Effectiveness of physical security is enhanced by:
  - strict key control, effective monitoring of electronic systems, accurate database management

Locks and Key Control

- Locks are mechanical devices consisting of a cylinder, springs, and several pins or tumblers the prevent rotation of the lock cylinder without the insertion of a correctly cut key.
- Proprietary systems have unique restricted key control duplication since they are only available to authorized users in agreement from authorized distributors.
- Restricted proprietary keyway combined with strict key control = Effective access control.

Key Control

- Management of keys should include a signature/receipt for issued keys.
- Each key should be stamped with a unique number.
- Temporary issue keys must be signed for and indicate a return time.
- When access privilege is revoked, keys should be retrieved and, if necessary, locks changed.
- Key control documentation should be considered as confidential and subject to similar record keeping procedures as the security register.

Electronic Access Control Systems

- Access is gained by presenting a card, badge, token, etc. to an access control reader.
- The reader is electronically connected to an access control network.
- Access authorization is determined when applied for.
- Unauthorized access attempt can raise an alarm directing security to take pre-determined actions.
- Used in the investigation of various incidents as well as monitoring time and attendance.

Access System Management Database

Granting and controlling access privileges must be governed by strict policies and procedure.

- Access to card holders should be strictly controlled.
- Access on the authorized people.
- Documentation should be protected.
- Documentation should be accessible.
- Pictures should be kept with files.
- Returned damaged or defective cards should be destroyed.
- Names should be pulled out of the database when the employee or contractor is no longer employed.
- Data entry must be consistently accurate.
- Confirmed through regular audits.

Biometric Technologies

- Increases level of access assurance only to authorized individuals.
- Requiring more that one factor is common in higher-security environments.
- Biometric systems include:
  - Hand, eye, voice and full facial recognition.
- CCTV facial recognition is used more by law enforcement.

Access Control in the Information Age

- Today, more organizations conduct business through networked arrangements.
- Access must be provided to employees and today a large number work from home
- As a result, this has provided adversaries with another avenue to gain unauthorized access.
- This threat had led to an increase in the IT Security field.
- The granting of on-line access must be controlled by strict policies and procedures.
- Continuous improvement and feedback so that ideas for change can be put forward by security personnel.
- Physical security must still be considered when developing an integrated security program.