

7. Physical Controls



14 Controls

- Physical control category aims to prevent unauthorized access
- Covers a range of controls related to physical security
- Includes prevention of unauthorized access to facilities
- Protects equipment and assets from damage or theft
- Includes management of physical security breaches
- Measures can include security guards, access control systems, locks, security, cameras
- Also includes secure storage and transportation of information
- Annex A recognizes importance of physical security in information security
- Helps ensure security and integrity of information and assets

Physical Controls (7.1-7.5)

7.1 Physical Security Perimeters: Prevent unauthorized physical access and damage to assets.

7.2 Physical Entry: Authorize physical access to protect organization's information

7.3 Securing Offices, Rooms and Facilities: Prevent unauthorized access and damage to assets.

7.4 Physical security monitoring: Prevent and identify unauthorized physical access

7.5 Protecting Against Physical and Environmental Threat: Prevent damage from physical and environmental threats



Physical Controls (7.6-7.10)



7.6 Working in Secure Areas: Protect secure areas and assets from internal damage and unauthorized access.



7.7 Clear Desk and Clear Screen: Minimize unauthorized access to info on desks/screens during and outside working hours.



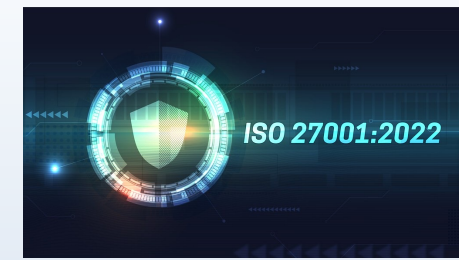
7.8 Equipment Siting and Protection: Minimize impact of physical, environmental threats and unauthorized access.

7.9 Security of Assets Off-premises: Protect organization from disruptions & unauthorized access to off-site devices.



7.10 Storage Media: Protect stored information from unauthorized access, modification, or destruction

Physical Controls (7.11-7.14)



7.11 Supporting Utilities: Prevent information loss or disruption due to utility failures

7.12 Cabling Security: Protect information, assets, and operations from cable-related issues

7.13 Equipment maintenance: Prevent damage, theft, compromise of assets and operational interruptions from maintenance neglect.

7.14 Secure Disposal or Reuse of Equipment: To avoid leakage of information when disposing or reusing equipment.

