ISO/IEC 27001:2013 Information security management systems
-Physical and environmental security – Secure areas-

Security category – 11.1. Physical and environmental security

Control – 11.1.1. Physical security perimeter
The organization should define and use security perimeters to protect areas that contain either sensitive or critical information and information processing facilities.

The premises of the organization may be at the risk of unauthorized access.

Guidelines for securing physical perimeters refer to:

- define perimeters and establish controls depending on the security requirements of the assets in each perimeter;
- ensure protection of the perimeters – doors, windows, roofs, walls, flooring;
- reception or similar area to control the physical access;
- fire doors should be alarmed, monitored and tested;
- intruder detection systems should be installed and unoccupied areas should be alarmed at all times.

Have multiple barriers or systems to prevent unauthorized access so the failure of one barrier does not compromise the security immediately.

ISO/IEC 27001:2013 Information security management systems
-Physical and environmental security – Secure areas-

Control – 11.1.2. Physical entry controls
There should be entry controls to ensure that only authorized personnel are allowed to access secure areas.

Guidelines for designing entry controls:

- date and time of entry and departure should be recorded;
- identity of the visitors should be confirmed and recorded;
- visitors should be supervised;
- access to areas where confidential information is processed or stored should be restricted to authorized individuals;
- all access should be logged;
- employees, contractors and external parties should wear visual identification; - external parties personnel should not be allowed to areas where confidential information is being processed (unless its critical and they should be monitored);
- physical access rights to areas should be reviewed regularly.

ISO/IEC 27001:2013 Information security management systems
-Physical and environmental security – Secure areas-

Control – 11.1.3. Securing offices, rooms and facilities
The organization should design and apply physical protection measures for offices, rooms and facilities.

Control measures for offices, rooms and facilities should be suitable to the value and importance of assets inside.

- key facilities should be sited to avoid access by the public;
- the organization should avoid the use of signs about the information processing facilities inside the rooms (ex. server room);
- Facilities should be configured to prevent confidential information or activities from being visible and audible from outside. Electromagnetic shielding may be needed;
- directories and phone books should not be readily accessible to anyone from outside the organization

ISO/IEC 27001:2013 Information security management systems
-Physical and environmental security – Secure areas-

Control – 11.1.4. Protecting against external and environmental threats
The organization needs to have physical protection against natural disasters, malicious attack or accidents.

Damage due to earthquake, fire, flooding, explosions, civil unrest or other forms of natural or man-made disasters.

For many of those in most countries there is specific legislation and ISO/IEC 27002 recommends the use of specialist advice on this matter

ISO/IEC 27001:2013 Information security management systems
-Physical and environmental security – Secure areas-

Control – 11.1.5. Working in secure areas
The organization should develop and use procedures for working in secure areas.

Secure areas - locations where critical information is being processed or stored, information that has great commercial value to the organization.

Guidelines for working in secure areas:

- personnel should only be aware of the existence of, or activities within a secure area on a need-to-know basis;
- only authorized personnel shall be allowed inside;
- unsupervised work in secure area should be avoided as much as possible and depending of course on the specifics of the area
- vacant secure areas should be locked and checked periodically
- photographic, video and audio recording equipment should not be allowed in secure areas unless specifically authorized.

ISO/IEC 27001:2013 Information security management systems
-Physical and environmental security – Secure areas-

Control – 11.1.6. Delivery and loading areas
Delivery and loading areas, as well as any other access points where unauthorized persons could enter the premises should be controlled and if its possible they should be isolated from the information processing facilities to avoid unauthorized access.

Uncontrolled access of public from outside can lead to security breaches.

Guidance on handling the security of delivery and loading areas include:

- delivery and loading areas should be designed so that delivery and loading personnel cannot access other parts of the building from those areas
- external doors of delivery and loading areas should be closed when internal doors that lead inside the organization are open
- If possible incoming material should be checked for explosives, chemicals or hazardous material before entering the delivery and loading area
- As much as possible it is recommended to segregate incoming and outgoing shipments
- Records of deliveries and dispatches should be kept (on paper or by video recording)