Physical entry

ISO 27002 Control 7.2

Control

Secure areas should be protected by appropriate entry controls and access points

Purpose

To ensure only authorized physical access to the organization's information and other associated assets occurs

Why is it important?

- It ensures accountability by tracking who accessed secure areas and when
- It prevents unauthorized access to premises containing information processing facilities
- It manages the specific risks posed by visitors and supplier personnel accessing secure areas

What should we take care of ?

- Access to entry points
- Authorized personnel only or accompanying visitors
- Entry log (identity, time of entry, time of exit)
- Areas containing information: access by card / biometrics / ...
- Staff presence at the entrance
- Visible badge
- Emergency exit protection
- Key management process
- Protection of loading areas
- Inventory of incoming/outgoing hardware

What could happen if badly implemented ?

- Unauthorized entry by staff, visitors, or delivery personnel
- Unauthorized access to secure areas or sensitive information processing facilities
- Security breach due to compromised physical keys or unauthorized access credentials

Link with other frameworks

- NIST 800-53 rev5 : PE-2, PE-3, PE-4, PE-5, PE-16
- NIST CSF 2.0 : ID.AM-08, PR.AA-06, PR.PS-03

Renaud Dardenne
Asphalia Consulting