Cabling security

ISO 27002 Control 7.12

Control

Cables carrying power, data or supporting information services should be protected from interception, interference or damage

Purpose

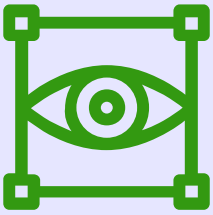
To prevent loss, damage, theft or compromise of information and other associated assets and interruption to the organization's operations related to power and communications cabling

Why is it important?

- Cabling is susceptible to accidental damage (e.g., cuts), intentional interference (e.g., interception, eavesdropping), and signal interference
- Adequate controls ensure confidentiality (preventing interception) and availability (preventing damage/cuts) of network services

How to put it in place ?

- Install power and telecommunications lines underground where possible or use alternative protection (e.g., armoured conduits)
- Segregate power cables from communications cables to prevent interference
- For sensitive systems, use electromagnetic shielding, alarms, and controlled access to patch panels/cable rooms
- Label cables at each end with source and destination details to enable physical identification



What to look for ?

- Cabling security
- Interception / Interference
- Power and telecommunications lines
- Electromagnetic shielding
- Fibre-optic cables

Link with other frameworks

- NIST 800-53 rev5 : PE-4, PE-9
- NIST CSF 2.0 : GV.OC-04, GV.OC-05, PR.AA-06, PR.IR-02

Renaud Dardenne
Asphalia Consulting