# ISO/IEC 27001:2013 Information security management systems
## *-Physical and environmental security – Equipment (1)-*

**Security category – 11.2. Equipment**

**Control – 11.2.1. Equipment sitting and protection**
*The equipment needs to be sited and protected from environmental threats and hazards and unauthorized access.*

***Equipment is vulnerable to damage, to unauthorized viewing and to interference.***

*Guidelines provided by ISO/IEC 27002:*
- equipment should be sited to minimize unnecessary access to work areas
- equipment where sensitive information is processed should be positioned so that the risk of information being viewed by unauthorized persons is reduced;
- controls should be in place to reduce the risk of physical or environmental threats;
- guidelines in place for eating, drinking and smoking;
- temperature and humidity should be monitored (if needed);
- use of special protection methods (ex. keyboard membranes) – if needed

# ISO/IEC 27001:2013 Information security management systems
## *-Physical and environmental security – Equipment (1)-*

**Control – 11.2.2. Supporting utilities**
*The organization should protect its equipment from power failures and other disruptions caused by failures in supporting utilities.*

***Supporting utilities include electricity supply, telecommunications, water supply, gas, sewage, ventilation, air conditioning, heating.***

A problem with any supporting utility should by identified by an alarm system.
Supporting utilities should be in line with the legal requirements and meet the needs of business growth.
They should be inspected regularly to ensure proper functioning.

Redundant connections for network connectivity should be obtained through the use of more than one provider.

# ISO/IEC 27001:2013 Information security management systems
## *-Physical and environmental security – Equipment (1)-*

**Control – 11.2.3. Cabling security**
*Power and telecommunications cabling carrying data or supporting information services should be protected from interception, interference of damage.*

***Guidelines for cabling security:***

- power and telecommunication lines should be underground where possible;
- power cables should be segregated from communication cables to prevent interference;
- for critical systems further controls include: armoured conduit and locked rooms or boxes at inspection and termination points; use of electromagnetic shielding of cables; controlled access to patch panels and cable rooms as well as inspection for unauthorized devices attached.

# ISO/IEC 27001:2013 Information security management systems
## *-Physical and environmental security – Equipment (1)-*

**Control – 11.2.4. Equipment maintenance**
*Equipment should be maintained to ensure its integrity and availability.*

***The guidelines for equipment maintenance:***

- respecting the supplier’s recommended service intervals and specifications;
- using only authorized maintenance personnel for repairs;
- clearing confidential information from the equipment scheduled for maintenance or verifying maintenance personnel (depending on the case);
- complying with the maintenance requirements in the insurance policies;
- before putting the equipment back in operation after maintenance ensuring that it has not been tampered with and does not malfunction.