Security of assets off-premises

ISO 27002 Control 7.9

Control

Off-site assets should be protected

Purpose

To prevent loss, damage, theft or compromise of off-site devices and interruption to the organization’s operations

Why is it important?

- Off-site assets are subject to higher risks of damage, theft, and eavesdropping than on-site equipment
- It ensures the security of information when working remotely
- For transferred equipment, an audit trail (chain of custody) is maintained

How can it be implemented ?

- Authorize the use of devices storing or processing information off-premises
- Implement guidelines to protect off-site equipment (e.g., not leaving them unattended, observing manufacturers' instructions)
- Implement location tracking and remote wiping capabilities
- For permanent installations (e.g., ATMs), implement physical security monitoring, environmental protection, and tamper proofing

What recurrent processes should be in place ?

- Devices used off-premises are secured according to guidelines
- A chain of custody log is maintained during transfer
- Location tracking and remote wiping capabilities are enabled and monitored where necessary

Link with other frameworks

- NIST 800-53 rev5 : AC-19, AC-20, MP-5, PE-17
- NIST CSF 2.0 : NA

Renaud Dardenne
Asphalia Consulting