User endpoint devices

ISO 27002 Control 8.1

Control

Information stored on, processed by or accessible via user endpoint devices should be protected

Purpose

To protect information against the risks introduced by using user endpoint devices

Why is it important?

- User endpoint devices are exposed to increased physical and network related threats outside the organization's secured premises
- Ensures that users are aware of their responsibilities for implementing security measures
- Necessary for managing risks associated with the use of personal devices (BYOD)

Which attributes are important ?

- Endpoint Management Policy
- Physical protection
- Software Installation Restrictions
- Inventory of installed applications
- Using the firewall
- Disk encryption
- Presence of antivirus
- Disabling storage USB ports
- Professional/personal separation
- Disabling insecure protocols

How can it be evidenced ?

- Documented topic-specific policy on secure configuration and handling of devices
- Configuration settings for user endpoint devices (e.g., encryption, screen locking features)
- Records of user acknowledgment of security duties (especially for BYOD)

Link with other frameworks

- NIST 800-53 rev5 : AC-11
- NIST CSF 2.0 : NA

Renaud Dardenne
Asphalia Consulting