Information deletion

ISO 27002 Control 8.10

Control

Information stored in information systems, devices or in any other storage media should be deleted when no longer required

Purpose

To prevent unnecessary exposure of sensitive information and to comply with legal, statutory, regulatory and contractual requirements for information deletion

Why is it important?

- Sensitive information should not be kept longer than required, reducing the risk of undesirable disclosure
- Ensures compliance with data retention laws
- Standard delete functions are inadequate for sensitive data
- Prevents unintentional exposure when equipment is returned to vendors

What do I have to do ?

- Select a deletion method in accordance with business requirements and relevant laws
- Delete sensitive information using approved, secure deletion software or physical destruction
- Log deletion results as evidence
- Include requirements for information deletion in third-party agreements
- Protect sensitive information by removing auxiliary storages before equipment leaves the premises

What should I not forget ?

- Systems delete information according to the retention policy
- Obsolete versions, copies, and temporary files are deleted
- Deletion results are recorded as official records
- Appropriate disposal mechanisms are used for different media types

Link with other frameworks

- NIST 800-53 rev5 : AC-4(25)*, AC-7(2)*, MA-2, MA-3(3)*, MA-4(3)*, MP-4, MP-6, MP-6(1)*, SI-21
- NIST CSF 2.0 : NA

Renaud Dardenne
Asphalia Consulting