Secure disposal or re-use of equipment

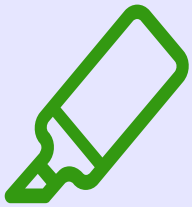
ISO 27002 Control 7.14

Control

Items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use

Purpose

To prevent leakage of information from equipment to be disposed or re-used



Why is it important?

- Information can be compromised through careless disposal or re-use of equipment
- It is necessary to remove sensitive data and licensed software before disposal or re-use
- It ensures the removal of security controls (e.g., access lists) if facilities are vacated

What are its sub controls ?

- Physically destroying storage media containing confidential information (or securely deleting content using non-retrievable techniques)
- Removing labels and markings identifying the organization, classification, or owner prior to disposal or re-use
- Performing a risk assessment on damaged equipment containing sensitive data to determine if physical destruction is necessary
- Considering full-disk encryption to reduce disclosure risk upon disposal

What small details are important ?

- Full-disk encryption reduces disclosure risk if the encryption process is sufficiently strong and keys are confidential (8.24)
- Secure overwriting tools should be applicable to the specific storage media technology
- Standard delete function is inadequate for confidential information

Link with other frameworks

- NIST 800-53 rev5 : MP-6
- NIST CSF 2.0 : ID.AM-08, PR.PS-03

Renaud Dardenne
Asphalia Consulting