ISO/IEC 27001:2013 Information security management systems
-Media handling-

RiG CERT

Security category – 8.3. Media handling

Control – 8.3.1. Management of removable media
Procedures should be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.

Removable media (flash disks, removable hard drives, CDs, DVDs, printed media, etc) containing the organization's data presents a vulnerability to loss of data and breaches of confidentiality.

Controls implemented have to address issues like:
- using removable media only if there is a business reason to do so;
- storing media in safe and secure environments;
- contents of re-usable media to be removed from the organization should be made unrecoverable;
- the organization may use encryption of data on removable media;
- transfer useful data on fresh media to prevent media degrading in time;
- have multiple copies of valuable information on separate media.

ISO/IEC 27001:2013 Information security management systems
-Media handling-

RiG CERT

> **Control – 8.3.2. Disposal of media**
> *When no longer needed media shall be disposed of according to procedures.*

Procedures for secure disposal reduce the risk of confidential information leakage to unauthorized persons.

ISO/IEC 27002 guidance on disposal of media:

- identify the items that require secure disposal;
- store and dispose securely media with confidential information (with methods like incineration, shredding, erasure of data - depending on the media);
- perform a careful selecting of the provider for collection and disposal services (if such a provider is used for the disposal of media);
- keep a log of the disposal of sensitive items.

ISO/IEC 27001:2013 Information security management systems
-Media handling-

Control – 8.3.3. Physical media transfer
Media that contains information has to be protected during transportation against unauthorized access, misuse or corruption.

Transportation of media = risks for loss, corruption, unauthorized access and misuse.

Guidelines for transportation of media:

- use of reliable couriers and make verification of courier identity
- use suitable packaging to protect the contents from physical damage and protection from environmental factors - like heat or electromagnetic fields;
- to mitigate the risk of breach of confidentiality if media are lost or stolen - data to be transported should be encrypted and of course the encryption key should never be sent together with the encrypted data.