ISO/IEC 27001:2013 Information security management systems
-Physical and environmental security – Equipment (2)-

Control – 11.2.5. Removal of assets
Taking equipment, information or software off-site should be done only with authorization.

The organization should have rules covering and a process to authorize taking assets out of the premises.

The rules regarding removal of assets may include aspects like:

- who authorizes taking assets out of premises;
- time limits for taking assets off premises;
- record the assets taken outside and the identity of the person(s).

Unauthorized removal of assets should be forbidden and employees need to be aware that spot checks can be done to verify this.

ISO/IEC 27001:2013 Information security management systems
-Physical and environmental security – Equipment (2)-

Control – 11.2.6. Security of equipment and assets off premises
Assets off-site should be protected taking into consideration the different risks involved by working outside the organization premises.

The use of equipment outside the premises involves many security threats.

When using equipment or media outside:

- it should not be left unattended in public places and it should be protected (according to its manufacturer specifications – ex. protection from electromagnetic fields)
- if the equipment is transferred between individuals there should be a log that defines the chain of custody.

ISO/IEC 27001:2013 Information security management systems
-Physical and environmental security – Equipment (2)-

Control – 11.2.7. Secure disposal or re-use of equipment
Before disposal or re-use, all equipment containing storage media shall be verified to ensure sensitive data and licensed software has been removed or securely overwritten.

Have controls in place to ensure that equipment to be disposed of or re-used does not contain sensitive information.

If storage media contains confidential or copyrighted information then this has to be securely deleted or overwritten so it can not be retrieved.
Consider destroying of media containing sensitive information as a method of disposal.

Simple deleting of files is usually not enough.

ISO/IEC 27001:2013 Information security management systems
-Physical and environmental security – Equipment (2)-

Control – 11.2.8. Unattended user equipment
Unattended equipment should be protected.

Unattended equipment may provide an opportunity for security breaches.

Users should be advised to:

- terminate active sessions when finished or secure them with a password;
- log-off from application or network services when no longer needed;
- use a lock system for all computers or mobile devices.

ISO/IEC 27001:2013 Information security management systems
-Physical and environmental security – Equipment (2)-

Control – 11.2.9. Clear desk and clear screen policy
The organization should develop and implement a clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities.

Defining and applying a clear desk/ clear screen policy reduces the risks of unauthorized access, loss and damage of information.

Guidelines on cs/cd policy include:
- sensitive or critical business information should be locked away preferably in a safe when not required and especially when the office is vacated
- computers should be logged off when unattended
- use of cameras and recording devices may be forbidden;
- media containing sensitive information should be removed from the printers after printing.