

ISO/IEC 27001:2013 Information security management systems

-Responsibility for assets-



Security category – 8.1. Responsibility for assets

Control – 8.1.1. Inventory of assets

The organization has to identify all assets associated with information and information processing facilities and should create and establish an inventory of assets.



The inventory is expected to include:

- physical assets - equipment identity, location, maker, model, serial number and inventory tag
- documentation - including system documentation, contracts, procedures and business continuity plans, etc
- software products - including licensing information and where they are used
- services - including utilities.

Asset inventory should be kept up to date.

ISO/IEC 27001:2013 Information security management systems

-Responsibility for assets-



Control – 8.1.2. Ownership of assets

Assets should have owners.

Ownership should be assigned to assets.

The asset owner (individual or entity) is responsible for the asset protection.

Asset owner should:

- ensure that asset is included in the inventory;
- ensure that the asset is appropriately protected;
- define and review access restrictions to the asset;
- ensure proper handling when the asset is deleted or destroyed.

ISO/IEC 27001:2013 Information security management systems

-Responsibility for assets-



Control – 8.1.3. Acceptable use of assets

The organization should identify, document and implement rules for the acceptable use of assets associated with information and information processing facilities

Individuals should be made aware of the security requirements associated with the assets and should be responsible for the use of the resources.

Organizations are vulnerable to misuse of their assets by employees – intentional or not – refers to use of assets in a way that is different than their business purposes.

There have to be rules describing the acceptable use of resources and users should be made aware of the rules and agree with them.

ISO/IEC 27001:2013 Information security management systems *-Responsibility for assets-*



Control – 8.1.4. Return of assets

Upon termination of employment, contract or agreement the users should return the assets belonging to the organization

Procedures should ensure assets are returned when the job is terminated.

If the employee purchases the organization's equipment or if it uses its own personal equipment for business purposes - rules should be in place to ensure that relevant information is transferred to the organization and the equipment is securely erased.