ISO/IEC 27001:2013 Information security management systems
-Information classification-

Security category – 8.2. Information classification

Control – 8.2.1. Classification of information
Information needs to be classified taking into consideration legal requirements, value of the information, criticality and sensitivity to unauthorized disclosure or modification.

The organization has to develop a classification scheme.
Owners of information assets are accountable for their classification.

Recommended to have an easy to understand classification scheme.

Classification should be done by taking into consideration the level of protection needed to ensure the confidentiality, integrity and availability of information.

The classification scheme has to be consistent across the whole organization.

ISO/IEC 27001:2013 Information security management systems
-Information classification-

ISO/IEC 27002 provides an example of classification scheme that uses 4 levels:

Public - disclosure causes no harm.

Internal use - disclosure causes minor embarrassment or minor operational inconvenience.

Confidential - disclosure has a significant short term impact on operations or tactical objectives.

Top secret - disclosure has a serious impact on long term strategic objectives or puts the survival of the organization at risk.

ISO/IEC 27001:2013 Information security management systems
-Information classification-

Control – 8.2.2. Labelling of information
Starting from the classification scheme the organization should develop procedures for the labelling of information.

Labelling reflect the level of classification.

Procedures for information labelling need to cover information and its related assets in physical and electronic formats.

Employees and contractors should be made aware of the labelling procedures.

When receiving information from other organizations - care should be given to the labels of documents as other organizations may have different definitions for same labels.

ISO/IEC 27001:2013 Information security management systems
-Information classification-

Control – 8.2.3. Handling of assets
The organization should implement procedures for the handling of assets in line with the classification scheme.

Procedures for asset handling are meant to prevent the risk of sensitive information being mishandled and should detail:

- access restrictions for each level of classification;
- protection of copies (temporary or permanent) in the same way as the originals;
- storage requirements according to the classification level;
- declassification and destruction according to classification