iGUIDE

ISMS

Information Security
Information Classification

iNFOSECBASE

Contents

A Guide to Information Classification

Introduction

Proper classification, handling and deletion of information are essential components of ISO 27001, ensuring that sensitive data is protected throughout its lifecycle. These processes help organisations manage information based on its value and sensitivity, mitigate risks of unauthorised access or disclosure and comply with legal, regulatory and contractual requirements.

By implementing clear policies and procedures for managing information, organisations can safeguard their assets, enhance operational efficiency and reduce the likelihood of data breaches. This guide outlines the key practices for effectively classifying, handling and securely deleting information in alignment with ISO 27001 standards.

Classification of Information

Classification ensures that information is categorised based on its value, sensitivity and criticality to the organisation.

Steps for Classification

Define Classification Levels

- Establish classification categories such as Public, Internal, Confidential or Restricted.
- Customise categories to suit organisational needs.

Identify Ownership

- Assign an information owner responsible for determining the classification of each asset.

Classify Information Assets

- Assess information based on its sensitivity, impact of disclosure and value to the organisation.
- Apply the appropriate classification level to all assets, including documents, databases and digital files.

Label Information

- Use consistent labels (e.g. Confidential or Restricted) to clearly indicate the classification of physical and digital information.
- Ensure that the information classifications are consistent throughout the ISMS.

Handling of Information

Proper handling ensures that information is used and accessed in accordance with its classification level.

Guidelines for Handling

Access Control

- Restrict access to information based on the principle of least privilege.
- Use strong authentication mechanisms for sensitive information.

Transmission

- Secure information during transmission using encryption or secure communication protocols.
- Verify recipient identities before sharing classified information.

Storage

- Store classified information in secure locations, such as locked cabinets or encrypted drives.
- Limit access to storage areas to authorised personnel only.

Usage

- Train employees on the proper handling of classified information.
- Monitor and log access to sensitive information to detect unauthorised activities.

Deletion and Disposal of Information

ISO 27001 requires organisations to securely delete or dispose of information when it is no longer needed to prevent unauthorised access or recovery.

Steps for Deletion and Disposal

Define Retention Periods

- Establish retention policies for different types of information.
- Ensure compliance with legal and contractual obligations regarding data retention.

Secure Deletion

- Use secure methods to permanently delete digital information, such as data-wiping tools or cryptographic erasure.
- Ensure backup copies are also deleted, if applicable.

Physical Disposal

- Shred or destroy physical documents containing sensitive information.
- Dispose of storage media, such as hard drives or USB devices, using certified destruction services.

Document Deletion Processes

- Maintain records of deletion and disposal activities to demonstrate compliance during audits.

Policies and Procedures

To ensure consistent practices, organisations should develop and implement policies and procedures that address classification, handling and deletion. These policies should:

- Define roles and responsibilities for managing information throughout its lifecycle.
- Outline processes for classifying, labelling and accessing information.
- Specify methods for securely deleting or disposing of information.
- Include training programs to ensure employees understand and comply with policies.

Benefits of Proper Classification, Handling and Deletion

- **Enhanced Security**: Reduces the risk of unauthorised access or disclosure of sensitive information.
- **Regulatory Compliance**: Ensures adherence to legal and contractual requirements for information protection.
- **Data Minimisation**: Prevents the unnecessary retention of information, reducing storage costs and risks.
- **Risk Reduction**: Mitigates threats associated with improperly managed or obsolete information.

Summary

By implementing robust practices for classification, handling and deletion of information, organisations can strengthen their ISMS, protect sensitive data and maintain compliance with ISO 27001 requirements. These practices also help build trust with stakeholders by demonstrating a commitment to effective information security management.

Effective classification, handling and deletion of information are critical aspects of ISO 27001, ensuring the protection of sensitive data throughout its lifecycle. Classification involves categorising information based on its value and sensitivity, while handling focuses on implementing appropriate measures for access, storage and transmission.

Secure deletion and disposal ensure that information no longer needed is permanently destroyed to prevent unauthorised recovery. By establishing clear policies and procedures for these processes, organisations can strengthen their ISMS, comply with legal and regulatory requirements and reduce the risk of data breaches.