iGUIDE

ISMS

Information Security Data Management

iNFOSECBASE

Contents

A Guide to Data Management

Introduction

ISO 27001 provides a robust framework for managing and securing information within an organisation. Data management is a critical component of this standard, ensuring that all data, whether personal, financial, operational or confidential, is handled, stored and protected in a secure and compliant manner throughout its lifecycle.

In an era where data is one of the most valuable organisational assets, effective data management ensures the confidentiality, integrity and availability of information, while safeguarding against breaches, loss and misuse.

ISO 27001 emphasises the importance of clear policies, robust controls and consistent monitoring to manage data securely and efficiently. This guide explores the principles and best practices of ISO 27001-compliant data management, highlighting how organisations can protect their information assets and ensure compliance with legal and regulatory requirements.

Importance of Data Management in ISO 27001

Effective data management ensures:

- Confidentiality, integrity and availability of data throughout its lifecycle.
- Compliance with regulatory frameworks such as GDPR, HIPAA or CCPA.
- Prevention of unauthorised access, data breaches or data loss.
- Clear accountability and processes for handling sensitive or critical information.

Key Principles of Data Management in ISO 27001

Data Classification

- Identify and classify data based on its sensitivity, value and regulatory requirements (e.g. public, internal, confidential or highly confidential).
- Use classification to guide security controls, such as encryption or access restrictions.

Data Handling

- Define clear policies and procedures for handling data, including collection, processing, sharing and disposal.
- Ensure that handling processes align with security and privacy regulations.

Data Storage and Retention

- Store data securely using appropriate controls such as encryption, backups and access control mechanisms.
- Establish and enforce data retention policies to ensure data is retained only as long as necessary and securely deleted when no longer required.

Access Control

- Implement role-based access control (RBAC) to limit access to data based on job responsibilities.
- Regularly review and update access permissions to prevent unauthorised access.

Data Integrity

- Ensure that data remains accurate, complete and consistent throughout its lifecycle.
- Use tools like checksums, hashes or version control to detect and prevent unauthorised modifications.

Data Backup and Recovery

Cyberattacks, system failures and human errors can wipe out critical data in seconds. Without a Backup Policy, your organisation risks permanent data loss, downtime and compliance violations. That's why ISO 27001 requires a structured approach to backups, ensuring data is securely stored and quickly recoverable when disaster strikes.

- Develop and implement a backup strategy to protect critical data against loss or corruption.
- Regularly test recovery procedures to ensure data can be restored in case of an incident.

What should a Backup Policy include?

- **Backup frequency and schedule**: Define how often critical data is backed up.
- **Storage locations and security**: Ensure backups are stored securely on-site and off-site.
- **Encryption and access control**: Protect backup data from unauthorised access.
- **Testing and validation**: Regularly test backups to ensure they work when needed.
- **Retention and recovery procedures**: Establish how long backups are kept and the process for restoring data.

Data Masking

Implementing data masking for some organisations may seem challenging, but it can be effectively managed by following a structured approach and leveraging third-party tools and services.

Data masking is typically required for sensitive and personally identifiable information (PII) to protect privacy, comply with regulations and reduce the risk of data breaches. Masked data should only be available to view, only as necessary, by authorised users. Below are common types of data that require masking:

- **Personally Identifiable Information (PII)**
  - Social Security Numbers (SSNs)
  - Passport numbers
  - Date of birth
  - Driver's license numbers
- **Financial Information**
  - Credit card numbers
  - Bank account numbers
  - Transaction details
  - Payment card data (PCI DSS requirements)
  - Taxpayer identification numbers
- **Health Information**
  - Medical records
  - Patient identifiers
  - Health insurance numbers
- **Authentication Information**
  - Usernames and passwords
  - Security questions and answers
  - Multi-factor authentication (MFA) data
- **Business-Sensitive Information**
  - Trade secrets
  - Intellectual property (IP) details
  - Proprietary algorithms
  - Research and development data
  - Pricing models
- **Customer and Vendor Data**
  - Account details
  - Communication records
  - Contract information

Data Leakage Prevention

To detect and prevent the unauthorised disclosure and extraction of information by individuals or systems, organisations must:

- Clearly identify and classify information
- Clearly define roles within the organisation for all parties involved. The role of each individual should be distinctly outlined to prevent data misuse by people with access to confidential information.
- Monitor data usage, access and logging; this provides an understanding of how data is used and identifies behaviours that put data at risk.

Data Management Lifecycle

Data Creation and Collection

- Establish guidelines for securely collecting and creating data.
- Ensure compliance with data protection laws during the collection process.

Data Use and Sharing

- Use secure methods for accessing and sharing data, such as encryption or secure file transfers.
- Ensure that sharing of data is limited to authorised individuals or third parties with appropriate agreements.

Data Archiving

- Archive data that is no longer actively used but needs to be retained for legal, historical or operational purposes.
- Secure archived data against unauthorised access.

Data Deletion and Disposal

- Define processes for securely deleting or disposing of data that is no longer needed.
- Use methods such as data wiping or physical destruction to ensure permanent deletion.

Best Practices for ISO 27001 Data Management

Develop a Data Management Policy

- Create a comprehensive policy outlining the organisation's approach to data classification, handling and protection.
- Ensure the policy is communicated to all employees and regularly reviewed.

Conduct Data Risk Assessments

- Identify and evaluate risks related to data storage, transfer and processing.
- Implement risk treatment plans to address identified vulnerabilities.

Monitor and Audit Data Activities

- Use logging and monitoring tools to track data access, modifications and transfers.
- Conduct regular audits to ensure compliance with policies and standards.

Provide Training and Awareness

- Train employees on data management policies, procedures and their individual responsibilities.
- Promote a culture of awareness regarding data security and privacy.

Secure Third-Party Data Management

- Ensure that third-party vendors handling organisational data comply with ISO 27001 and other relevant standards.
- Include data protection clauses in contracts and regularly assess vendor compliance.

Benefits of ISO 27001-Compliant Data Management

- **Enhanced Data Security**: Protects sensitive information from breaches, loss or unauthorised access.

- **Regulatory Compliance**: Ensures alignment with data protection laws and industry standards.
- **Improved Operational Efficiency**: Establishes clear guidelines for handling, storing and disposing of data.
- **Stakeholder Trust**: Builds confidence in the organisation's ability to manage and protect information.
- **Risk Reduction**: Identifies and mitigates risks related to data management.

Summary

ISO 27001-compliant data management ensures the secure handling, storage and disposal of information throughout its lifecycle. By focusing on data classification, secure storage, access control, retention policies and proper disposal, organisations can protect the confidentiality, integrity and availability of their data.

Key practices include developing clear policies, conducting risk assessments, monitoring data activities and providing employee training. Effective data management also ensures compliance with legal and regulatory requirements, reduces risks and builds stakeholder trust. With ISO 27001, organisations can create a robust framework for managing and safeguarding their information assets.

By implementing robust data management practices, organisations can safeguard their information assets and build a resilient information security framework.