iGUIDE

ISMS

Information Security
Use of Cryptography

iNFOSECBASE

Contents

A Guide to Information Security Use of Cryptography

Introduction

Cryptography is a fundamental component of information security, ensuring confidentiality, integrity and authenticity of sensitive data. ISO 27001:2022 defines cryptographic controls under A.8.24: Use of Cryptography, emphasising its role in protecting data at rest, in transit and during processing. Proper implementation of cryptographic measures helps organisations secure communications, comply with regulations and prevent unauthorised data access.

This guide provides an overview of the use of cryptography, its objectives, key requirements and best practices for effective cryptographic implementation.

Use of Cryptography

Objective

To ensure that cryptographic controls are properly implemented and managed to protect sensitive information from unauthorised access, disclosure and tampering.

Key Requirements

- Define a cryptographic policy that outlines how encryption is applied across the organisation.
- Identify which data and systems require cryptographic protection based on risk assessments.
- Use strong encryption algorithms that comply with industry standards.
- Implement secure key management practices to prevent unauthorised access to encryption keys.
- Ensure cryptographic controls align with legal, regulatory and contractual requirements.

Implementation Best Practices

Cryptographic Policy and Governance

- Develop a formal cryptographic policy specifying when and how encryption is used.
- Define roles and responsibilities for managing cryptographic operations.
- Ensure compliance with regulations such as GDPR, PCI DSS and NIST standards.

Data Encryption Best Practices

- Encrypt data at rest using AES-256 for files, databases and storage devices.
- Secure data in transit with TLS 1.2 or TLS 1.3 for web communications, VPNs and email encryption.
- Use end-to-end encryption (E2EE) for sensitive communications.
- Implement full-disk encryption (FDE) on laptops and mobile devices.

Key Management and Security

- Use a Key Management System (KMS) to generate, store and rotate encryption keys securely.
- Enforce key rotation policies to prevent long-term exposure of encryption keys.
- Protect keys with Hardware Security Modules (HSMs) or cloud-based secure key vaults.
- Implement multi-factor authentication (MFA) for key access.

Cryptographic Algorithm Selection

- Use industry-approved encryption standards (AES, RSA, ECC, SHA-256).
- Avoid outdated or vulnerable algorithms like MD5, SHA-1 and RC4.
- Ensure post-quantum cryptographic readiness for future security resilience.

Compliance and Auditing

- Regularly audit cryptographic implementations to identify vulnerabilities.
- Ensure cryptographic controls align with regulatory requirements and contractual obligations.
- Document cryptographic processes to facilitate compliance reviews and risk assessments.

Benefits of Using Cryptography in ISO 27001:2022

Implementing cryptographic controls provides several security and compliance benefits, including:

Data Confidentiality: Ensures that sensitive data is accessible only to authorised users.

Data Integrity: Prevents unauthorised modifications to data through cryptographic hashing.

Authentication and Non-Repudiation: Uses digital signatures and certificates to verify identities.

Regulatory Compliance: Meets security requirements under ISO 27001, GDPR, HIPAA and PCI DSS.

Risk Reduction: Minimises the impact of data breaches by rendering stolen data unreadable.

Summary

The Use of Cryptography in ISO 27001plays a critical role in protecting sensitive information from unauthorised access and cyber threats. Organisations must implement strong encryption mechanisms, secure key management practices and compliance-driven cryptographic policies to ensure the security and integrity of their data. By adopting best practices such as AES-256 encryption, TLS-secured communications and HSM-based key management, businesses can enhance data protection, meet regulatory requirements and safeguard their digital assets against emerging threats.