iGUIDE

ISMS

Information Security Acceptable Use

iNFOSECBASE

Contents

A Guide to Information Security Acceptable Use of Information and Other Associated Assets

Introduction

In ISO 27001, defining the acceptable use of information and other associated assets is crucial for ensuring the secure and responsible handling of an organisation's data, IT systems and digital resources.

An Acceptable Use Policy (AUP) establishes clear guidelines on how employees, contractors and third parties can access, use and protect company assets; it helps prevent security incidents, data breaches and misuse while ensuring compliance with legal, regulatory and contractual requirements.

By implementing a well-structured policy, organisations can promote responsible behaviour, reduce security risks and safeguard critical information.

Importance of Acceptable Use in ISO 27001

The Acceptable Use Policy is essential for:

- **Defining Responsibilities**: Clarifies what users can and cannot do with company resources.
- **Preventing Security Risks**: Reduces the likelihood of unauthorised access, data leaks and cyber threats.
- **Ensuring Compliance**: Aligns with legal, regulatory and industry security standards.
- **Protecting Organisational Assets**: Prevents misuse of IT systems, networks and sensitive data.

Key Elements of an Acceptable Use Policy

An ISO 27001-compliant Acceptable Use Policy should include:

Purpose and Scope

- Defines the objectives of the policy and its importance in maintaining information security.
- Specifies who the policy applies to (employees, contractors, third parties etc.).

Authorised Use of Information and IT Resources

- Clarifies permitted use of company data, systems, email, internet and cloud services.
- Outlines business-related and personal use limitations.

Access Control and User Responsibilities

- Requires users to follow strong password policies and multi-factor authentication (MFA).
- Prohibits sharing login credentials and unauthorised system access.

Data Protection and Confidentiality

- Defines how sensitive information should be handled, stored and transmitted.
- Enforces encryption, data classification and secure disposal practices.

Use of Internet, Email and Communication Tools

- Establishes rules for using company email, instant messaging and social media.
- Prohibits accessing inappropriate content or engaging in illegal activities.

Prohibited Activities

- Restricts downloading unauthorised software or accessing malicious websites.
- Forbids using company resources for personal financial gain or unauthorised data sharing.

Reporting Security Incidents

- Requires users to report suspicious activities, phishing attempts and data breaches immediately.
- Provides guidelines for incident escalation and response.

Consequences of Non-Compliance

- Outlines disciplinary actions for policy violations, including warnings, access revocation or legal consequences.

Best Practices for Implementing an Acceptable Use Policy

Clearly Define and Communicate the Policy

- Ensure all employees understand their responsibilities through clear, concise language.
- Distribute the policy during onboarding and require acknowledgment.
- Provide Regular Security Awareness Training
- Conduct training sessions on secure data handling, phishing threats and password management.
- Reinforce acceptable use guidelines through ongoing awareness campaigns.

Enforce Policy Compliance

- Implement monitoring tools to detect policy violations (e.g. unauthorised access, data transfers).
- Use automated alerts and periodic audits to assess compliance.

Regularly Review and Update the Policy

- Update the policy to reflect new security risks, regulatory changes and technology advancements.
- Conduct an annual review as part of the organisation's ISO 27001 compliance process.

Integrate with Other ISO 27001 Controls

- Align the Acceptable Use Policy with access controls, cryptographic controls and incident management.

Benefits of an ISO 27001-Compliant Acceptable Use Policy

- **Enhanced Security Awareness**: Reduces risks of human error, which is a leading cause of security incidents.
- **Stronger Regulatory Compliance**: Meets data protection requirements e.g. GDPR, HIPAA etc.
- **Minimised Cyber Threats**: Helps to prevent malware infections, unauthorised access and data breaches.
- **Improved Operational Efficiency**: Ensures employees use IT resources productively and securely.
- **Legal Protection**: A well-documented AUP can protect a business from potential legal liabilities by ensuring that the organisation meets legal and compliance requirements.

Summary

An ISO 27001-compliant Acceptable Use Policy provides a framework for secure and appropriate use of organisational information and IT resources. It defines authorised access, user responsibilities, data protection measures and prohibited activities while enforcing compliance through monitoring and incident reporting.

Regular training, policy enforcement and periodic updates help maintain security awareness and effectiveness.

By implementing a strong acceptable use policy, organisations enhance cybersecurity, ensure regulatory compliance and reduce risks associated with unauthorised data access and misuse.