# ISO 27001-Compliant Acceptable Use Procedure Template

## Introduction

This Acceptable Use Procedure aligns with ISO 27001 standards, providing a framework for the secure and responsible use of organizational assets, including laptops, email systems, cloud storage, information systems, devices, and data. The procedure ensures that all users understand and adhere to practices that protect the confidentiality, integrity, and availability of information assets.

## Purpose

The purpose of this procedure is to define clear guidelines for the acceptable use of organizational assets to minimize risks associated with misuse, unauthorized access, or data breaches. This contributes to maintaining a secure and compliant operational environment.

## Scope

This procedure applies to all users of organizational assets, including:

* Employees
* Contractors
* Temporary staff
* Third-party vendors and partners with access to organizational resources

## Policy Statement

The organization is committed to ensuring the secure and responsible use of its assets by:

* Defining acceptable and prohibited activities when using organizational assets. Examples of prohibited activities include accessing unauthorized websites, installing unapproved software, and sharing login credentials.
* Ensuring compliance with applicable laws, regulations, and internal policies.
* Protecting assets from unauthorized access, loss, or damage.
* Educating users on their responsibilities and the potential consequences of misuse.

The procedure includes the following six steps:

1. Asset Identification: Define the organizational assets covered under this procedure, such as devices, systems, and data.
2. Access Control: Ensure access to assets is limited to authorized users based on their roles and responsibilities.
3. Usage Guidelines: Provide clear instructions on acceptable and prohibited activities, including restrictions on personal use and downloading unauthorized software.
4. Monitoring and Auditing: Implement monitoring systems to track asset usage and detect unauthorized activities.
5. Incident Response: Establish procedures for reporting and addressing incidents of misuse or policy violations.
6. Review and Training: Regularly review the procedure and provide training to users on acceptable use policies.

## Roles and Responsibilities

* Information Security Officer: Ensures the procedure aligns with ISO 27001 requirements and oversees compliance.
* IT Operations Team: Implements technical controls to enforce acceptable use policies and monitors system usage.
* HR Department: Collaborates with the IT Operations Team to communicate acceptable use guidelines during onboarding, ensures acknowledgment of the procedure, and coordinates training programs to keep users informed of policy updates.
* All Users: Adhere to the acceptable use guidelines and report any incidents or security concerns.

## Compliance and Monitoring

Compliance with this procedure will be ensured through:

* Regular audits of system usage logs to detect violations.
* Monitoring compliance with key performance indicators (KPIs), such as:

- Percentage of users who have completed acceptable use training.

- Number of incidents involving acceptable use violations.

Non-compliance incidents will be documented, and corrective actions will be implemented. Repeat violations may result in disciplinary actions, including revocation of access or termination.

## Related Documentation

* Information Security Policy
* Access Control Policy
* Incident Response Plan
* Employee Handbook

## Review and Revision

This procedure will be reviewed annually or when significant changes occur in technology, regulatory requirements, or organizational policies. The Information Security Officer will initiate the review process, and updates will be communicated to all stakeholders. All updates will be documented and approved through a formal review process.

## Narrative Guidance

This procedure provides a comprehensive framework for the acceptable use of organizational assets. It emphasizes the importance of user awareness and accountability in maintaining a secure environment. Organizations are encouraged to adapt this template to reflect specific operational and regulatory needs.

## Instructions for Use

* Replace placeholders with organization-specific details.
* Ensure alignment with related policies and standards.
* Collaborate with stakeholders to address unique requirements and operational contexts.