# Bring Your Own Device (BYOD) Procedure Template

## Introduction

The Bring Your Own Device (BYOD) Procedure establishes guidelines and controls to manage the use of personal devices for accessing organizational systems and data, ensuring compliance with the organization’s information security policies and ISO 27001 standards. This procedure seeks to mitigate risks associated with personal device usage while supporting operational flexibility and productivity.

## Purpose

The purpose of this procedure is to define clear requirements for the secure use of personal devices within the organization, ensuring that such usage does not compromise the confidentiality, integrity, and availability of organizational data.

## Scope

This procedure applies to all employees, contractors, and third-party users who wish to use their personal devices to access organizational systems, applications, or data. It includes smartphones, tablets, laptops, and other personal computing devices.

## Policy Statement

The organization permits the use of personal devices for business purposes under the following conditions:  
  
Examples of acceptable use:  
- Accessing organizational email and collaboration tools through approved applications.  
- Using personal devices to securely access the organization's virtual private network (VPN) for work-related tasks.  
  
Examples of unacceptable use:  
- Storing sensitive organizational data locally on personal devices without encryption.  
- Using unauthorized software or applications to access organizational systems.  
  
1. Personal devices must be registered and approved before accessing organizational systems.  
2. Approved security software must be installed and maintained on personal devices.  
3. Users must adhere to the organization’s Acceptable Use Policy and other relevant guidelines.  
4. The organization reserves the right to revoke access or wipe organizational data from personal devices if security policies are breached or the device is lost.

## Roles and Responsibilities

- Device Owners:  
 - Ensure their devices meet the organization’s security requirements.  
 - Report lost, stolen, or compromised devices immediately.  
- IT Department:  
 - Define and communicate technical requirements for personal devices.  
 - Manage the registration, approval, and revocation of BYOD access.  
- Managers:  
 - Approve or deny BYOD requests for team members based on business needs.  
- Information Security Team:  
 - Monitor compliance with BYOD security policies and conduct periodic audits.

## Procedure Steps

1. Request and Registration:  
 - Users submit a BYOD access request form, detailing the device type and intended use.  
 - IT reviews the request and verifies that the device meets technical and security standards.  
  
2. Approval and Setup:  
 - Approved devices are configured with required security software, including mobile device management (MDM) solutions.  
 - Users sign an agreement acknowledging BYOD policies and responsibilities.  
  
3. Access Management:  
 - IT grants access to organizational systems, ensuring appropriate permissions are assigned based on user roles.  
  
4. Monitoring and Compliance:  
 - IT and Information Security periodically review BYOD activity to ensure policy adherence.  
 - Non-compliant devices are flagged, and corrective actions are initiated.  
  
5. Incident Response:  
 - In case of device loss, theft, or security compromise, users report the incident to IT immediately.  
 - IT remotely disables access or wipes organizational data from the device if necessary.  
  
6. Revocation:  
 - Access is revoked upon employment termination or if the user opts out of the BYOD program.  
 - Users must ensure all organizational data is removed from their devices before revocation.

## Compliance and Monitoring

Compliance with this procedure is enforced through:  
- Regular audits of BYOD devices and their configurations.  
- Monitoring access logs for unusual or unauthorized activity.  
- Ensuring adherence to ISO 27001 requirements and organizational security policies.

## Related Documentation

- Information Security Policy  
- Acceptable Use Policy  
- Incident Response Procedure  
- Data Protection Policy

## Review and Revision

This procedure is reviewed annually by the Information Security Manager in collaboration with the IT Department. Changes are made as required to align with evolving technological, regulatory, and organizational needs.

## Narrative Guidance

This procedure supports ISO 27001 by ensuring secure access to information systems through personal devices. It also addresses risks related to unauthorized access, data leakage, and device security, aligning with the organization’s broader information security management framework.