# Identity Access Management Procedure Template

## Introduction

This Identity Access Management (IAM) Procedure outlines the framework for managing and controlling access to organizational systems, applications, and data. In alignment with ISO 27001 standards, this procedure ensures the confidentiality, integrity, and availability of information through robust access controls.

## Purpose

The purpose of this procedure is to establish a systematic approach for granting, modifying, and revoking access to organizational resources. By implementing stringent identity and access controls, the organization aims to minimize security risks, prevent unauthorized access, and ensure compliance with regulatory and business requirements.

## Scope

This procedure applies to all employees, contractors, and third-party users requiring access to organizational resources. It encompasses all systems, applications, and data managed by the organization.

## Policy Statement

1. Access Request and Approval: Access to systems and resources must be formally requested and approved by authorized personnel based on business needs.  
2. Role-Based Access Control (RBAC): Access privileges must align with defined roles and follow the principle of least privilege. Roles and privileges should be defined based on job responsibilities and documented in an access control matrix. This matrix must be regularly updated to reflect changes in roles, responsibilities, or organizational structure.  
3. Authentication Mechanisms: Multi-factor authentication (MFA) must be implemented for accessing critical systems and sensitive information. Examples of MFA mechanisms include hardware tokens, authenticator apps (such as Google Authenticator or Microsoft Authenticator), and biometric authentication like fingerprint or facial recognition.  
4. Access Review and Audit: Access rights must be reviewed periodically to ensure continued relevance and compliance.  
5. Termination of Access: Access to systems and resources must be promptly revoked upon employee termination or role change.  
6. Monitoring and Logging: All access to critical systems must be logged and monitored for suspicious activities.

## Roles and Responsibilities

- System Owners: Approve access requests and conduct periodic access reviews for their respective systems.  
- IT Department: Implement and manage IAM tools, enforce access controls, and monitor access logs.  
- HR Department: Notify the IT department of employee terminations or role changes requiring access updates.  
- Compliance Officer: Conduct periodic audits to ensure adherence to IAM procedures and alignment with ISO 27001 standards.

## Compliance and Monitoring

Compliance with this procedure will be monitored through:  
- Regular access reviews and audits.  
- Automated alerts for unauthorized access attempts.  
- Periodic reports on IAM metrics and incidents.  
Non-compliance will result in corrective actions as defined in the organization’s disciplinary policy.

## Related Documentation

- Information Security Policy  
- Acceptable Use Policy  
- Incident Management Procedure  
- Data Classification Policy

## Review and Revision

This procedure will be reviewed annually or in response to significant changes in IAM tools, organizational structure, or regulatory requirements. Updates will be approved by the Information Security Steering Committee.

## Narrative Guidance

This document reflects the organization’s commitment to ISO 27001. Adherence to this procedure ensures that access to information and systems is granted and managed in a secure and compliant manner, thereby reducing the risk of data breaches and unauthorized activities.