# Annual System Access Review Procedure Template

## Introduction

The Annual System Access Review Procedure outlines the systematic process for conducting annual reviews of system access to ensure compliance with the organization’s information security policies and ISO 27001 standards. This procedure supports the principle of least privilege and aims to safeguard sensitive information and assets by ensuring that access rights remain appropriate and justified.

## Purpose

The purpose of this procedure is to define a structured approach to reviewing system access rights, ensuring they align with current roles and responsibilities, and identifying and rectifying any deviations. This promotes the security and integrity of the organization’s information systems.

## Scope

This procedure applies to all employees, contractors, and third-party users with access to the organization’s systems, applications, and data. It encompasses all information systems classified as critical or sensitive as per the organization’s information classification policy.

## Policy Statement

The organization mandates an annual review of all system access rights to confirm their appropriateness and compliance with the principle of least privilege. Failure to adhere to this mandate could result in unauthorized access, increased security risks, and potential non-compliance with regulatory and contractual obligations. The review must:  
1. Validate that access rights correspond to current job roles and responsibilities.  
2. Identify and revoke access no longer required.  
3. Ensure compliance with regulatory, legal, and contractual obligations.

## Roles and Responsibilities

- System Owners: Responsible for initiating and overseeing the annual access review process for systems under their control.  
- Managers: Validate that team members’ access rights align with their roles and responsibilities.  
- Access Review Coordinator: Coordinates the review process, compiles access reports, and tracks completion status.  
- Internal Audit Team: Verifies compliance with this procedure and reports any discrepancies.

## Procedure Steps

1. Initiation: The Access Review Coordinator notifies System Owners to commence the review process, providing guidance and deadlines.  
 - Generate and distribute access reports for each system.  
  
2. Validation: System Owners and Managers review the access reports, verifying:  
 - Each user’s access rights.  
 - Alignment with current roles and responsibilities.  
  
3. Revocation: Identify and document users whose access should be revoked or modified. Ensure that changes are implemented promptly.  
  
4. Approval: Document the validation process, including sign-offs from Managers and System Owners confirming the appropriateness of access rights.  
  
5. Audit and Compliance: Internal Audit Team reviews the completed access review documentation to ensure compliance with this procedure and ISO 27001 standards.  
  
6. Reporting: The Access Review Coordinator compiles a final report summarizing findings, actions taken, and outstanding issues, if any, for management review.

## Compliance and Monitoring

Compliance with this procedure is monitored through:  
- Regular internal audits to verify adherence to the review timeline.  
- Random sampling of access review records to ensure accuracy and completeness.  
- Annual reviews by the Information Security Committee to identify improvement opportunities.

## Related Documentation

- Information Security Policy  
- Access Control Policy  
- Information Classification Policy  
- Internal Audit Procedure

## Review and Revision

This procedure is reviewed annually by the Information Security Manager in consultation with relevant stakeholders. Updates are made as required to address changes in regulations, organizational requirements, or ISO 27001 standards.