# Hiring Procedure Template

## Introduction

This Hiring Procedure provides a structured approach to recruiting and onboarding employees, ensuring alignment with ISO 27001 standards. It emphasizes securing sensitive information, validating candidate qualifications, and maintaining compliance with organizational and legal requirements.

## Purpose

The purpose of this procedure is to outline the process for hiring personnel who meet the organization’s standards and align with its security objectives. This ensures that only qualified and trustworthy individuals are granted access to organizational resources, reducing the risk of insider threats and safeguarding sensitive information.

## Scope

This procedure applies to all hiring activities, including full-time, part-time, and contract positions. It encompasses candidate evaluation, background checks, and onboarding processes for all roles within the organization.

## Policy Statement

1. Job Description Creation: Each position must have a clearly defined job description outlining the required qualifications, responsibilities, and security obligations.  
2. Candidate Screening: All candidates must undergo a thorough screening process, including identity verification, professional reference checks, and, where applicable, criminal background checks.  
3. Interview Process: Interviews must assess both technical qualifications and alignment with the organization’s security culture. For example, interviewers may ask candidates to describe how they have handled sensitive information in past roles, or how they ensure compliance with security policies in their day-to-day activities. Role-specific scenario-based questions can also be used to evaluate their understanding of security practices.  
4. Employment Agreement: All new hires must sign a confidentiality agreement and an acknowledgment of the organization’s security policies.  
5. Access Provisioning: Access to systems and facilities must be granted based on the principle of least privilege, ensuring only necessary access for their role.  
6. Onboarding Training: New employees must complete mandatory training on security policies and procedures before being granted access to organizational resources.

## Roles and Responsibilities

- Hiring Managers: Define job descriptions, oversee interviews, and ensure compliance with this procedure.  
- HR Department: Conduct candidate screenings, manage employment agreements, and facilitate onboarding processes.  
- IT Department: Implement access controls and ensure system access aligns with role-specific requirements.  
- Compliance Officer: Oversee alignment with ISO 27001 standards and conduct periodic audits of the hiring process.

## Compliance and Monitoring

Compliance with this procedure will be monitored through:  
- Regular audits of hiring records and practices.  
- Verification of completed background checks and signed confidentiality agreements.  
- Reviews of access provisioning to ensure adherence to the principle of least privilege.  
Non-compliance will result in corrective actions as per the organization’s disciplinary policy.

## Related Documentation

- Information Security Policy  
- Access Control Policy  
- Data Protection Policy  
- Training and Awareness Procedure

## Review and Revision

This procedure will be reviewed annually or in response to significant changes in hiring practices, organizational structure, or regulatory requirements. Revisions will be approved by the Compliance and HR departments.

## Narrative Guidance

This document supports the organization’s compliance with ISO 27001 emphasizing secure practices in pre-employment, during employment, and post-employment stages. Adhering to this procedure ensures that the organization’s workforce aligns with its security and compliance objectives.