# ISO 27001 Hiring Guideline Template

## Introduction:

This document outlines the Hiring Guideline Process for [COMPANY NAME], aligned with ISO 27001 requirements. It ensures that the recruitment, onboarding, and management of personnel align with the organization’s Information Security Management System (ISMS). These guidelines are designed to safeguard information assets and minimize risks associated with human resources.

## 1. Purpose of the Hiring Guidelines

The purpose of this process is to:  
1. Ensure personnel with appropriate qualifications and trustworthiness are hired.  
2. Protect the organization’s information assets by verifying candidates’ background and integrity.  
3. Mitigate risks related to personnel handling sensitive information.  
4. Maintain compliance with legal, regulatory, and contractual obligations.  
5. Foster a security-aware culture through onboarding and training.

## 2. Recruitment Workflow Diagram

Diagram: Insert a graphical workflow diagram depicting the recruitment process, from job posting to onboarding.

## 3. Pre-Employment Requirements

* Job Description: Define roles and responsibilities, including specific security-related responsibilities.
* Candidate Screening: Conduct thorough background checks (e.g., criminal record checks, employment history verification).
* Risk Assessment for Roles: Assess security risks associated with roles involving access to sensitive data or systems.
* Non-Disclosure Agreement (NDA): Require candidates to sign an NDA to protect confidential information.
* Security Awareness Assessment: Evaluate candidates’ understanding of basic security principles.

## 4. Onboarding Process

* Policy Acknowledgment: Require new hires to review and acknowledge the Information Security Policy.
* Initial Training: Provide mandatory security awareness training covering topics like data handling, incident reporting, and secure communication.
* Access Provisioning: Grant access based on the principle of least privilege, maintaining a log of assigned access rights.
* Asset Allocation: Assign necessary assets (e.g., laptops, badges) and document them in the Asset Register.

## 5. Employment Period Requirements

* Ongoing Training: Schedule periodic refresher training on information security topics.
* Performance Monitoring: Evaluate compliance with security policies during performance reviews.
* Access Reviews: Conduct regular reviews of access rights to ensure alignment with job responsibilities.
* Incident Reporting: Provide mechanisms for employees to report policy violations or security concerns anonymously.

## 6. Termination or Role Change Process

* Exit Interviews: Conduct interviews to remind employees of their NDA obligations.
* Access Revocation: Immediately revoke access to all systems and assets upon termination or role change.
* Asset Recovery: Ensure all physical and digital assets are returned.
* Data Preservation: Preserve necessary organizational data before deactivating accounts.
* Final Review: Use a checklist to verify the completion of all offboarding tasks.

## 7. Metrics for Hiring Guidelines

* Percentage of employees completing onboarding training within the first month.
* Number of security incidents involving new hires within the first 90 days.
* Frequency of access reviews for current employees.
* Percentage of terminated employees completing all offboarding tasks.

## 8. Roles and Responsibilities

Human Resources (HR):  
- Oversee recruitment and onboarding.  
- Ensure compliance with background screening and legal requirements.

Information Security Manager (ISM):  
- Provide input on security responsibilities for job descriptions.  
- Develop and deliver security awareness training.

Hiring Managers:  
- Define job-specific security responsibilities.  
- Evaluate candidates’ suitability and trustworthiness.

IT Operations Team:  
- Assign and monitor access rights and assets.  
- Revoke access during offboarding.

## 9. Revision and Maintenance

This document and the Hiring Guideline Process will be reviewed [Insert frequency, e.g., annually or as needed] to ensure alignment with organizational priorities, regulatory requirements, and industry best practices.

## Approval:

| Name | Title | Date |
| --- | --- | --- |
|  |  |  |
|  |  |  |