Human Resources Security Policy Template

Document Control Information

- **Document Title:** Human Resources Security Policy
- **Document Version:** 1.0
- **Last Updated:** [DATE]
- **Document Owner:** [ROLE/NAME]
- **Approved By:** [ROLE/NAME]
- **Next Review Date:** [DATE]

1. Introduction

1.1 Purpose

This Human Resources Security Policy establishes [ORGANIZATION NAME]'s approach to managing information security risks associated with human resources before, during, and after employment in accordance with ISO 27001:2022 requirements. It provides a framework for ensuring that employees and contractors understand their responsibilities and are suitable for their roles.

1.2 Scope

This policy applies to: - All employees, including full-time, part-time, and temporary staff - All contractors, consultants, and third-party personnel - All stages of the employment lifecycle, including recruitment, onboarding, employment, and termination - All roles and responsibilities related to information security - All locations where work is performed, including remote work

1.3 Policy Statement

[ORGANIZATION NAME] is committed to: - Ensuring that employees and contractors understand their information security responsibilities - Verifying that employees and contractors are suitable for their roles - Protecting the organization's information assets throughout the employment lifecycle - Promoting a culture of security awareness and compliance - Addressing security concerns related to human resources promptly and effectively

2. Pre-Employment

2.1 Security in Job Descriptions

- Information security responsibilities shall be included in job descriptions
- Required security skills and qualifications shall be specified
- Security clearance requirements shall be defined where applicable
- Handling of sensitive information shall be addressed
- Compliance with security policies shall be included as a responsibility

2.2 Screening and Background Checks

- Background verification checks shall be conducted for all candidates
- Checks shall be proportional to the business requirements and role
- Checks shall comply with relevant laws and regulations
- Checks may include:
    - Identity verification
    - Employment history verification
    - Educational and professional qualification verification
    - Criminal record checks (where legally permitted)
    - Credit checks (for financially sensitive positions)
    - Reference checks
- Results of checks shall be documented and securely stored
- Adverse findings shall be assessed for security implications

2.3 Terms and Conditions of Employment

- Information security responsibilities shall be included in employment contracts
- Confidentiality or non-disclosure agreements shall be signed
- Intellectual property rights shall be addressed
- Data protection responsibilities shall be specified
- Consequences of non-compliance shall be clearly stated
- Terms shall apply both during and after employment
- Contractors shall have equivalent terms in their agreements

3. During Employment

3.1 Management Responsibilities

- Management shall require employees to comply with security policies
- Management shall ensure employees receive appropriate security training
- Management shall set a good example for security practices
- Management shall monitor compliance with security requirements

- Management shall address security violations promptly
- Management shall provide feedback on security performance

3.2 Information Security Awareness and Training

- Security awareness training shall be provided to all personnel
- Training shall be provided during onboarding and regularly thereafter
- Training shall cover:
    - Security policies and procedures
    - Correct use of information assets
    - Security responsibilities
    - Common threats and vulnerabilities
    - Incident reporting procedures
- Role-specific security training shall be provided where needed
- Training effectiveness shall be evaluated
- Training records shall be maintained

3.3 Disciplinary Process

- A formal disciplinary process shall be established for security violations
- The process shall be fair, proportional, and consistently applied
- The process shall consider:
    - Nature and severity of the violation
    - Impact on the organization
    - Whether it was a first offense or repeated behavior
    - Training and awareness provided
    - Relevant legislation
- The process shall be communicated to all employees
- Disciplinary actions shall be documented
- The process shall respect privacy and confidentiality

4. Change of Employment

4.1 Job Changes and Transfers

- Security responsibilities shall be reviewed when roles change
- Access rights shall be updated to reflect new responsibilities
- Additional security training shall be provided if required
- Confidentiality agreements shall be updated if necessary
- Knowledge transfer shall include security aspects
- Previous access rights shall be removed if no longer required

4.2 Performance Management

- Security compliance shall be included in performance evaluations
- Security objectives shall be established where appropriate
- Security incidents shall be considered in performance reviews
- Positive security behaviors shall be recognized and rewarded
- Security improvement needs shall be addressed through training
- Performance issues related to security shall be addressed promptly

5. Termination or Change of Employment

5.1 Termination Responsibilities

- Security aspects of termination shall be defined and assigned
- HR, IT, and Security teams shall coordinate termination processes
- Managers shall oversee the return of assets and removal of access
- Employees shall be reminded of ongoing confidentiality obligations
- Knowledge transfer shall be completed before departure
- Exit interviews shall include security aspects

5.2 Return of Assets

- All organizational assets shall be returned upon termination
- Assets may include:
    - Computing devices and mobile equipment
    - Storage media and documents
    - Access cards and keys
    - Credit cards and financial instruments
    - Software and licenses
- Asset return shall be documented and verified
- Unreturned assets shall be reported and addressed

5.3 Removal of Access Rights

- All access rights shall be removed or modified upon termination
- Access removal shall include:
    - Network and system accounts
    - Email and communication systems
    - Physical access to facilities
    - Remote access capabilities
    - Cloud services and applications
    - Third-party services
- Shared accounts and passwords shall be changed

- Access removal shall be verified and documented
- Emergency access procedures shall be updated if necessary

5.4 Final Security Briefing

- Departing personnel shall receive a final security briefing
- Ongoing security obligations shall be explained
- Confidentiality requirements shall be reinforced
- Return of assets shall be confirmed
- Questions or concerns shall be addressed
- Contact information for security matters shall be provided

6. Remote and Mobile Working

6.1 Remote Work Security

- Security requirements for remote work shall be defined
- Remote work shall be authorized and documented
- Remote work environments shall meet security standards
- Secure communication methods shall be used
- Information handling guidelines shall be provided
- Remote work security shall be regularly assessed

6.2 Mobile Device Security

- Security requirements for mobile devices shall be defined
- Mobile device usage shall comply with the Mobile Device Policy
- Security controls shall be implemented on mobile devices
- Data on mobile devices shall be protected
- Lost or stolen devices shall be reported immediately
- Mobile device security shall be regularly assessed

7. Third-Party Personnel

7.1 Contractor and Third-Party Requirements

- Security requirements shall be defined for third-party personnel
- Contracts shall include security responsibilities
- Third-party personnel shall receive security awareness training
- Access shall be limited to necessary systems and information
- Third-party personnel shall be identified distinctly from employees
- Third-party compliance shall be monitored

7.2 Outsourced Development

- Security requirements shall be defined for outsourced development
- Secure development practices shall be required
- Code reviews and security testing shall be performed
- Intellectual property rights shall be protected
- Source code security shall be maintained
- Development environments shall be separated from production

8. Security Awareness and Culture

8.1 Security Culture Development

- A positive security culture shall be promoted
- Security leadership shall be visible and engaged
- Security successes shall be recognized and celebrated
- Security shall be integrated into business processes
- Security communication shall be regular and effective
- Security feedback shall be encouraged and addressed

8.2 Security Communications

- Regular security communications shall be provided
- Communications shall be clear and relevant
- Multiple channels shall be used for communications
- Communications shall address current threats and issues
- Security alerts shall be promptly distributed
- Communication effectiveness shall be measured

9. Confidentiality and Non-Disclosure

9.1 Confidentiality Agreements

- Confidentiality agreements shall be required for all personnel
- Agreements shall be signed before access to sensitive information
- Agreements shall clearly define confidential information
- Agreements shall specify protection requirements
- Agreements shall include duration of obligations
- Agreements shall be legally reviewed and enforceable

9.2 Intellectual Property Protection

- Intellectual property rights shall be protected

- Ownership of work products shall be clearly defined
- Use of third-party intellectual property shall be controlled
- Intellectual property protection shall be included in training
- Violations shall be addressed through the disciplinary process
- Legal remedies shall be pursued when necessary

10. Roles and Responsibilities

10.1 Human Resources Department

- Implement security measures in HR processes
- Coordinate background verification
- Include security in employment contracts
- Maintain confidentiality of personnel information
- Coordinate termination processes
- Support security training and awareness

10.2 Information Security Team

- Define security requirements for HR processes
- Provide security awareness materials
- Support security incident investigations
- Monitor compliance with security policies
- Advise on security aspects of HR issues
- Coordinate access management

10.3 Managers and Supervisors

- Ensure staff compliance with security policies
- Include security in performance management
- Support security training and awareness
- Report security incidents and concerns
- Manage access rights for their teams
- Coordinate termination security processes

10.4 All Personnel

- Comply with security policies and procedures
- Protect information assets
- Maintain confidentiality of information
- Report security incidents and weaknesses
- Complete required security training
- Return assets upon termination

11. Compliance and Monitoring

11.1 Compliance Verification

- Compliance with this policy shall be regularly verified
- Verification methods may include:
  - Internal audits
  - Self-assessments
  - Management reviews
  - Security awareness assessments
- Non-compliance shall be addressed through appropriate channels
- Compliance trends shall be analyzed and reported

11.2 Policy Exceptions

Exceptions to this policy shall be: - Documented with justification - Risk-assessed and approved by appropriate management - Time-limited and regularly reviewed - Accompanied by compensating controls where appropriate

12. Related Documents

- Information Security Policy
- Acceptable Use Policy
- Mobile Device and Remote Working Policy
- Access Control Policy
- Disciplinary Procedure
- Confidentiality Agreement Template
- [LIST OTHER RELEVANT POLICIES AND PROCEDURES]

13. Approval

This Human Resources Security Policy is approved by:

Name: _______________________ Position: _____________________ Date: ________________________ Signature: ____________________