# Human Resources Security Policy

To use this template, simply replace the text in dark grey with information customized to your organization. When complete, delete all introductory or example text and convert all remaining text to black prior to distribution.

|  |  |
| --- | --- |
| **Policy Owner** | Name the person/group responsible for this policy’s management. |
| **Policy Approver(s)** | Name the person/group responsible for implementation approval of this policy. |
| **Related Policies** | Name other related enterprise policies both within or external to this manual. |
| **Related Procedures** | Name other related enterprise procedures both within or external to this manual. |
| **Storage Location** | Describe physical or digital location of copies of this policy. |
| **Effective Date** | List the date that this policy went into effect. |
| **Next Review Date** | List the date that this policy must undergo review and update. |

# Purpose

Describe the factors or circumstances that mandate the existence of the policy. Also state the policy’s basic objectives and what the policy is meant to achieve.

The purpose of this policy is to ensure personnel, including contractors, are aware of and understand their responsibilities in regards to security.

# Scope

Define to whom and to what systems this policy applies. List the employees required to comply, or simply indicate “all” if all must comply. Also indicate any exclusions or exceptions, i.e. those people, elements, or situations that are not covered by this policy or where special consideration may be made.

This Human Resource Security Policy applies to all business processes and data, information systems, as well as components, personnel, and physical areas of [Insert Company’s Name].

# Definitions

Define any key terms, acronyms, or concepts that will be used in the policy. A standard glossary approach is sufficient.

# Governing Laws & Regulations

If applicable, list any laws or regulations that govern the policy or with which the policy must comply. Confirm with the legal department that the list is full and accurate. If there are no pertinent governing laws or regulations, delete this section.

|  |  |
| --- | --- |
| **Guidance** | **Section** |
| ISO27001:2013 | A.7.1, A.7.2., A.7.3 |
| NIST SP 800-53 v4 | XX-1 controls, PL-4, PS-2, PS-3, PS-6, PS-7, SA-21, PM-13, PM-14, AT-2, AT-3, CP-3, IR-2, SA-16, PS-8, PS-4, PS-5, AC-2, PE-2, PS-4, PS-5 |

# Policy Statements

Describe the rules that comprise the policy. This typically takes the form of a series of short prescriptive and proscriptive statements. Sub-dividing this section into sub-sections may be required depending on the length or complexity of the policy.

**Prior to Employment:**

* All candidates for employment, including contractors and third-party users, must undergo background verification checks in accordance with the appropriate laws.
* Contractual agreements with all employees and contractors will clearly outline the responsibility of the individual/contractor to information security.
  + Responsibilities will be reviewed and updated regularly.

**During Employment:**

* Management must require and ensure all employees and contractors adhere to applicable information policies and procedures within the organization.
  + - This includes access agreements which must be signed by personnel prior to being granted access.
      * Access agreements will be reviewed and updated regularly.
  + All employees and contractors must undergo awareness training based on their roles, as well as relevant updates in policies and procedures applicable to their jobs.
    - [Insert Company’s Name] management should require employees, contractors, and third-party users to apply security in accordance with established policies and procedures of the organization.
    - Training must be accompanied by an assessment procedure based on the cyber security training content presented in order to determine comprehension of key cyber security concepts and procedures.
  + If there is a failure to comply with these security requirements, there will be a formal, communicated process to take action against said employee(s) or contractor(s).

**Termination and Change of Employment:**

* In the event of an employee’s termination or transfer of employment, formal and communicated disciplinary actions must be taken.
  + This process includes exit interviews and removal of documents (and all copies thereof) and other [Insert Company’s Name] property and materials in their possession or control.

**Relevant Procedures**

Consider creating formal procedure documents that reinforce and support the policy statements above. Note, it is best practice to house policies and procedures in separate documents to keep the content focused and reduce the number of times the policy must be reapproved by senior management.

# Non-Compliance

Clearly describe consequences (legal and/or disciplinary) for employee non-compliance with the policy. It may be pertinent to describe the escalation process for repeated non-compliance.

Violations of this policy will be treated like other allegations of wrongdoing at [Company Name]. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable [Company Name] policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements.