# Personnel Security Policy

Version [Revision #]

Last modified: [Last modified date]

Last reviewed: [Last reviewed date]

Last Approval: [Last approval date]

#### *Disclaimer*

*This policy template is created as a useful resource. However, organizations remain fully responsible for the content of their policies. Every organization is unique, and the content and format of this template must be revised to meet your organization’s specific requirements. The set of templates available from Hyperproof is not exhaustive nor inclusive; your organization may choose to use only a portion of them or to split them into multiple policies. Do not rely on this policy template to meet legal, regulatory, or contractual requirements. Review your policy in detail to ensure that it is appropriately tailored to your organization's business objectives and legal requirements.*

### Security boundary under scope

1. [List of applicable systems]

### References

1. ISO/IEC 27001:2022: A.5.11, A.5.18, A.6.1, A.6.2, A.6.4, A.6.5
2. NIST 800-53 rev. 5: AC-2(13), AC-2(2), AC-2(3), PL-4, PL-4(1), PS-1, PS-2, PS-3, PS-4, PS-5, PS-8
3. PCI DSS 4.0: 3.7.8, 8.2.5, 12.4.2, 12.4.2.1, 12.7.1
4. AICPA SOC 2 TSC: CC1.1, CC1.4, CC1.5, CC3.3, CC6.2, CC6.3, CC6.4
5. CIS v8: 6.2, 15.7

## Document ownership

 <(Choose from)>

* 1. Policy Owner:
		1. [Owner name] ([Owner email]), [Owner title]
	2. Information Security Officer:
		1. [Information officer name], ([Information officer email]), [Information officer title]
	3. System Owner(s):
		1. [System owner name], ([System owner email]), [System owner title]
	4. Process and Operational Owner(s)
		1. [process owner], ([process owner email]), [process owner title]
	5. System Administrator(s):
		1. [System admin name], ([System admin email]), [System admin title]
	6. Required Dissemination: <(Choose from)>
		1. IT Administrator
		2. Engineering
		3. Product Management
		4. Support
		5. Information Security Team
		6. [Organization name] Leadership Team
		7. Contractors
		8. Vendors
		9. Company Wide
		10. [Organization name] SIRT
	7. Optional Dissemination: <(Choose from)>
		1. IT Administrator
		2. Engineering
		3. Product Management
		4. Support
		5. Information Security Team
		6. [Organization name] Leadership Team
		7. Contractors
		8. Vendors
		9. Company Wide
		10. [Organization name] SIRT

## Purpose

The purpose of the Personnel Security Policy is to establish a comprehensive framework for ensuring the security and integrity of the organization's human resources. This policy aims to safeguard the organization's assets, protect sensitive information, and maintain a secure and compliant working environment by defining the standards and procedures for managing employees and contractors throughout their tenure. It addresses key aspects such as screening and background checks, terms of employment, training, acceptable use, policy enforcement, and the processes for termination and transfer of personnel.

## Scope

This policy applies to all employees and contractors of the organization, including full-time, part-time, temporary, and remote workers. It encompasses all stages of employment, from pre-employment screening and onboarding to ongoing training, daily operations, and eventual termination or transfer. The policy outlines the responsibilities of various departments, including Human Resources, Information Security, and Legal, in ensuring compliance with these standards. It also covers all types of sensitive information and assets that employees and contractors may interact with, ensuring a holistic approach to personnel security within the organization.

## Roles and responsibilities

<(choose from)>

| **Role** | **Person &/or Title** | **Responsibility** |
| --- | --- | --- |
| Plan and Policy Management | [Owner name], [owner title] | Establish the controls, implementation, and monitoring strategy for [policy topic] and associated policy and procedure |
| Executive Review | Executive Team | Adjusts [policy topic] parameters to meet business requirements and appropriate risk appetite. Approves risk model and supporting risk documentation that applies to the [policy topic] Policy. Reads, understands and approves after appropriate editing, the [policy topic] Policy. |
| Approval and Commitment | Executive Team | Responsible for approval, and commitment to information security controls. Members of the leadership team of [Organization] to include [list of executive approvers]. |
| Information System Owner | [Information officer name], [Information officer title] | Responsible for the overall implementation, development, integration, modification, or operation and maintenance of configuration management. Develops operational strategies and tactics to comply with configuration management policy in coordination with the information systems administrators, the information security officer, and functional “end users.” |
| Operations | [Operational owner], Operational owner title] |  |
| Information Systems Administrators | System Administrators  | Effectively manages the daily implementation, monitoring, and maintenance of operational security controls, as directed by the System Owner and Information Security Officer. |
| Human Resource | [HR name], [HR title] | Setups HR wellbeing strategies, coordinates travel policy across the organization. Initiates emergency travel considerations, including crisis management when required. |
| End Users |  End Users | Users of information systems are required to comply with policy and procedures in the [policy topic] policy. |
| Providers | [provider type] | [provider service description] |

## Management commitment

* 1. [Organization] executive management affirms its commitment to the establishment, implementation, resourcing, monitoring, and effectiveness of [policy topic] controls and policy
	2. Management has reviewed and approved this policy.
	3. This policy demonstrates management's commitment to maintaining adequate controls as part of its information security management and privacy objectives. These objectives include compliance with applicable laws, regulatory requirements, executive orders, industry best practices, standards, guidelines, and contractual commitments.
	4. Management agrees to regularly review and update this policy to ensure that it effectively meets the organization’s business and compliance objectives.

## Coordination among organizational entities

1. The [responsible group] creates policy and procedure and is responsible for overall configuration management.
2. Policy and procedures will be reviewed, modified, and disseminated to required consumers.
3. The [responsible group] is responsible for coordinating documentation review and updating the policy.
4. The [responsible group] is responsible for communicating the policy and procedures to applicable required and optional parties.
5. The [responsible group] is responsible for training applicable required and optional parties on compliance with the policy and procedures.

## Compliance

* 1. Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties.
	2. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties

## Definitions

* 1. Acceptable Use Policy (AUP): A set of rules and guidelines that defines how employees and contractors may use the organization's information systems, resources, and data.
	2. Access Permissions: The rights and privileges granted to users to access and interact with the organization's systems, data, and resources.
	3. Artificial Intelligence (AI) Policy: Guidelines that regulate the use and application of AI technologies within the organization, ensuring ethical and secure usage.
	4. Background Check: The process of verifying the personal, professional, and financial history of a potential employee or contractor to assess their suitability for a position.
	5. Confidentiality Agreement: A legal contract between the organization and an employee or contractor that outlines the obligation to keep certain information private and secure.
	6. Disciplinary Process: The procedures and actions taken by the organization in response to violations of policies or misconduct by employees or contractors.
	7. Employee Handbook: A comprehensive document provided to employees and contractors that outlines the organization's policies, procedures, and expectations.
	8. Information Security (InfoSec): Measures and controls implemented to protect the confidentiality, integrity, and availability of the organization's information systems and data.
	9. Information Security Training Program: A structured program designed to educate employees and contractors about the organization's information security policies, practices, and their individual responsibilities.
	10. Non-Compete Agreement: A contract that restricts an employee or contractor from engaging in business activities that compete with the organization during and after their employment.
	11. Non-Disclosure Agreement (NDA): A legal contract that prohibits employees or contractors from disclosing confidential information belonging to the organization.
	12. Role-Based Training: Specialized training provided to employees and contractors based on their specific job functions and access levels within the organization.
	13. Screening: The process of evaluating the qualifications, background, and suitability of potential employees and contractors before hiring.
	14. Termination Process: The procedures followed by the organization to formally end an employee's or contractor's employment, including revoking access and retrieving company assets.
	15. Transfer Process: The procedures followed when an employee or contractor changes roles within the organization, including updating access permissions and reallocating assets.

## Policy

#### Screening and Background Checks

The [responisble party] shall:

* + 1. Conduct thorough pre-employment screening and background checks for all potential employees and contractors based on the risk of the position
		2. Verify identity, work history, education, and relevant certifications as determined by the risk of the position
		3. Perform criminal background checks against industry-standard databases
		4. Document and securely store all screening results.
		5. Ensure that screening processes comply with relevant laws and regulations

#### Terms of Employment

The [responsible party] shall:

* + 1. Clearly outline terms of employment in offer letters and contracts.
		2. Include job descriptions, salary, benefits, work hours, and conditions of employment.
		3. Ensure all employment terms comply with relevant laws and regulations.
		4. Develop and maintain an Employee Handbook detailing company policies, procedures, and expectations.
		5. Require all employees and contractors to acknowledge receipt and understanding of the Employee Handbook in writing.

#### Non-Disclosure and Other Agreements

The [responsible party] shall:

* + 1. Draft and enforce Non-Disclosure Agreements (NDAs) for all employees and contractors with access to protected data
		2. Ensure all relevant parties sign Confidentiality Agreements and Non-Compete Agreements where appropriate.
		3. Regularly review and update agreements to reflect current legal and business requirements.

#### Information Security and Role-Based Training

The [responsible party] shall:

* + 1. Maintain a policy for Information Security and Role-based Training
		2. Develop and implement a comprehensive Information Security Training Program for all employees and contractors.
		3. Provide role-based training specific to the responsibilities and access levels of personnel.
		4. Require all employees and contractors to complete initial training upon hire and participate in ongoing training sessions annually.

#### Acceptable Use and AI Policy

The [responsible party] shall:

* + 1. Establish an Acceptable Use Policy detailing the proper use of company assets, third-party software, and services.
		2. Develop an AI Policy outlining the acceptable use of artificial intelligence tools and services, including restrictions and responsibilities.

#### Policy Enforcement and Disciplinary Actions

The [responsible party] shall:

* + 1. Enforce compliance with all personnel security policies.
		2. Establish a clear disciplinary process for policy violations, ranging from warnings to termination.
		3. Document all incidents of non-compliance and actions taken.

#### Termination Process

The [responsible party] shall:

* + 1. Clearly communicate termination decisions to affected employees and contractors.
		2. Revoke all access to company systems, accounts, and physical premises upon termination within a reasonable period, as determined by the risk of the position
		3. Ensure the return of all company assets, including hardware, software, documents, and access badges.
		4. Securely disable accounts and remove access permissions in all relevant systems.

#### Transfer Process

The [responsible party] shall:

* + 1. Properly communicate role changes and transfers to affected employees and their managers.
		2. Review and update access and permissions in alignment with new roles and responsibilities.
		3. Ensure the return and reallocation of company assets as necessary.
		4. Document all changes and maintain accurate records of asset transfers and access modifications.

## Policy exemptions

* 1. Requests for exceptions to this policy shall be reviewed by the [exemption officer 1] and the [exemption officer 2] and/or the [responsible group].
	2. Employees requesting exceptions shall provide such requests to [exemption communication channel].
	3. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the [responsible group], initiatives, actions, and a timeframe for achieving the minimum compliance level with the policies set forth herein.

## Related documents

* 1. [list of related documents, including:
		1. Policies
		2. Procedures
		3. Standards
		4. Documentation
		5. Regulations
		6. Legal context

]

## Revision history

* 1. This policy is reviewed and, if necessary, updated annually and may also be updated to reflect changes in the environment.
	2. Every change to this plan must be reviewed and evidence of review and acceptance noted with a signature below. This plan requires the signature of: <(choose from)>
		1. The Information Security Officer
		2. Officer of the [Organization name] Leadership Team
	3. All changes requiring approval must be communicated to the required parties

| **Rev. #** | **Revision Date** | **Description** | **Author** | **Owner** | **Exec. reviewer** |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |

## Approval history

| **Step** | **Approver** | **Job Function** | **Signature** | **Approval Date** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |