|  |  |
| --- | --- |
| **[Organization Name]**  **Information Technology Standard** | **No:** [Policy Number: e.g. POL-GOV-01] |
| **IT Standard**:  **Personnel Security Policy** | **Updated:** [Updated Date] |
| **Issued By:** [Authority: e.g. CEO or CIO]  **Owner:** [Owner: e.g. IT Department] |

# 1.0 Purpose and Benefits

The purpose of this cybersecurity personnel policy is to establish safeguards that ensure only authorized personnel have access to the organization's IT resources and data. By assigning risk designations, performing personnel screening, managing terminations and transfers, and enforcing access agreements, this policy aims to mitigate risks associated with human interactions in IT environments. It ensures that proper security measures are in place, protecting the confidentiality, integrity, and availability of sensitive organizational information while supporting compliance with industry standards and best practices.

# 2.0 Authority

This policy is established under the authority of organizational management and is guided by best practices outlined in the National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0. While not mandated by law, the organization adopts this framework to enhance its cybersecurity posture and protect its information assets. The authority for enforcement and adherence to this policy is vested in the [Authority], who is responsible for ensuring compliance across all departments.

# 3.0 Scope

This policy applies to users of any system’s information or physical infrastructure regardless of its form or format, created or used to support the organization. It is the user’s responsibility to read and understand this policy and to conduct their activities in accordance with its terms. In addition, users must read and understand the organization’s Information Security Policy and its associated standards.

# 4.0 Information Statement

This policy establishes the necessary security measures to protect the organization’s IT resources by managing personnel-related risks. It applies to all departments, users, and third-party personnel with IT access. Key provisions include assigning risk designations to all positions, screening and rescreening individuals prior to system access, and revoking access upon termination. The policy also outlines requirements for managing personnel transfers and ensuring access agreements are signed and updated regularly. Exit interviews ensure that security obligations, such as nondisclosure, are understood upon termination, and security-related assets are retrieved.

Third-party providers must comply with the organization’s security policies, with IT monitoring adherence to these standards. Violations of security policies trigger a formal sanction process, ensuring that appropriate measures are taken in cases of non-compliance. This policy ensures robust personnel security practices are in place, contributing to the overall protection of sensitive organizational information and IT systems.

### Position Risk Designation

Information Technology (IT) shall:

* 1. Assign a risk designation to all positions.
  2. Establish screening criteria for individuals filling those positions.
  3. Review and update position risk designations [entity defined frequency].

### Personnel Screening

1. Screen individuals prior to authorizing access to the information systems.
2. Rescreen individuals according to [entity defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of such rescreening].
3. Ensure personnel screening and rescreening activities reflect applicable state and federal laws, directives, regulations, policies, standards, guidance, and specific criteria established for the risk designations of assigned positions.

### Personnel Termination

1. Disable information system access within [entity defined time period].
2. Terminate/revoke any authenticators/credentials associated with the individual.
3. Conduct exit interviews that include a discussion of [entity defined information security topics].
4. Retrieve all security-related information system-related property.
5. Retain access to information and information systems formerly controlled by terminated individual.
6. Notify [entity defined personnel or roles] within [entity defined time period].

Information system-related property includes, for example, hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes. Exit interviews ensure that terminated individuals understand the security constraints imposed by being former employees and that proper accountability is achieved for information system-related property. Security topics of interest at exit interviews can include, for example, reminding terminated individuals of nondisclosure agreements and potential limitations on future employment. Exit interviews may not be possible for some terminated individuals.

1. The entity shall notify terminated individuals of applicable, legally binding post-employment requirements for the protection of information.
2. The entity shall require terminated individuals to sign an acknowledgment of post-employment requirements as part of the termination process as directed by Counsel and Human Resources (HR).
3. The entity shall employ automated mechanisms to notify [entity defined personnel or roles] upon termination of an individual.

### Personnel Transfer

Departments shall:

1. Review and confirm ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions.
2. Initiate [entity defined transfer or reassignment actions] within [entity defined time period following the formal transfer action].
3. Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer.
4. Notify [entity defined personnel] within [entity defined time period] of transfer.

This control applies when reassignments or transfers of individuals are permanent or of such extended durations as to make the actions warranted.

### Access Agreements

Departments shall:

1. Develop and document access agreements for information systems.
2. Review and update the access agreements [entity defined frequency].
3. Ensure that individuals requiring access to information and information systems:
4. Sign appropriate access agreements prior to being granted access.
5. Re-sign access agreements to maintain access to information systems when access agreements have been updated or [entity defined frequency].

Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements.

### Access Agreements Third-Party Personnel Security

[Owner] shall:

1. Establish and document personnel security requirements including security roles and responsibilities for third-party providers.
2. Require third-party providers to comply with personnel security policies and procedures established by the entity.
3. Require third-party providers to notify [entity defined personnel] of any personnel transfers or terminations of third-party personnel who possess credentials and/or badges, or who have information system privileges within [entity defined time-period].
4. Monitor provider compliance.

Third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management.

### Personnel Sanctions

[Owner] Department shall:

1. Employ a formal sanction process for individuals failing to comply with established information security policies and procedures
2. Notify [entity defined personnel] within [entity defined time period] when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.
3. Sanction processes reflect applicable state and federal laws, directives, regulations, policies, standards, and guidance. Sanctions processes are described in access agreements and can be included as part of general personnel policies and procedures for those organizations.

# 5.0 Compliance

This policy shall take effect upon publication. Compliance is expected with all enterprise policies and standards. Policies and standards may be amended at any time; compliance with amended policies and standards is expected.

If compliance with this standard is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, entities shall request an exception through the following process.

# 6.0 Policy Exceptions

Requests for exceptions to this policy must be submitted to the [Authority] by the requesting department. Each request should include the scope and justification for the exception, potential risks, proposed mitigation measures, and a timeframe for achieving compliance. The [Authority] will review and discuss these requests with the department.

# 7.0 Definitions of Key Terms

|  |  |
| --- | --- |
| **Term** | Definition |
|  |  |

# 8.0 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

[Organization Address & Policy Owner’s Contact Info]

# 9.0 Revision History

This standard shall be subject to periodic review to ensure relevancy.

| **Date** | **Description of Change** | **Reviewer** |
| --- | --- | --- |
|  |  |  |

# 10.0 Related Documents

[National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53a – Personnel Security (PS)](https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final)

[National Institute of Standards and Technology (NIST) Special Publication 800-12, An Introduction to Information Security](https://csrc.nist.gov/pubs/sp/800/12/r1/final)

[National Institute of Standards and Technology (NIST), The NIST Cybersecurity Framework (CSF) 2.0](https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf)