|  |  |
| --- | --- |
| [Organization Name] | **No:**  [Policy Number] |
| **IT Policy**:  **Personnel Security** | **Updated:** 10/26/2024 |
| **Issued By:**  [Policy Authority]  **Owner:**  [Policy Owner] |

# 1.0 Purpose and Benefits

Risk management is a critical component of any information security program. It helps ensure that any risk to confidentiality, integrity, and availability is identified, analyzed, and maintained at acceptable levels. Risk assessments allow management to prioritize and focus on areas that pose the greatest impact to critical and sensitive information assets. This provides the foundation for informed decision-making regarding information security.

Federal and State mandates require routine assessments to identify risk and ensure appropriate controls. Risk assessments allow alignment of information security with business objectives and regulatory requirements. Identifying information security risk and considering control requirements from the onset is essential, and far less costly than retrofitting or addressing the impact of a security incident.

This standard provides a risk management framework to evaluate current security posture, identify gaps, and determine appropriate actions.

# 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 [Policy Authority], who is responsible for ensuring compliance across all departments.

# 3.0 Scope

This policy applies to all employees, contractors, third-party vendors, and any individuals or entities accessing, using, or managing the organization's information systems, networks, and physical infrastructure, regardless of the medium or format of the information. It covers all electronic, paper-based, and verbal communication, including, but not limited to, data processing systems, cloud services, email platforms, mobile devices, databases, and other digital storage mechanisms that store, transmit, or process sensitive organizational information.

The policy encompasses internal and external users, whether they access the organization's systems on-site or remotely, and includes all physical infrastructure such as data centers, workstations, and hardware that interact with or support the organization's information environment. Additionally, it extends to any devices, both personal and organizational, that connect to the corporate network or handle company data.

All users are responsible for protecting the confidentiality, integrity, and availability of information, complying with this policy and relevant laws, and familiarizing themselves with the organization's security policies and procedures to ensure the protection of organizational assets. Failure to comply with these requirements may result in disciplinary action, including termination of access rights or contractual agreements.

# 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.

* 1. Position Risk Designation

The [Policy Owner] 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 annually.
   1. Personnel Screening

The [Policy Owner] shall:

1. Screen individuals prior to authorizing access to the information systems.
2. Rescreen individuals under at least the following conditions
   1. Change in Job Role: Rescreening may be required when an individual changes to a position with different access privileges or responsibilities.
   2. Suspicion of Misconduct: If there are credible allegations or indications of misconduct, a rescreening may be warranted.
   3. Periodic Review: Regular intervals (e.g., every two years) as part of a standard review process.
   4. Regulatory Changes: If new laws or regulations come into effect that affect background check requirements or security clearances.
   5. Major Organizational Changes: During significant organizational shifts, such as mergers or acquisitions, that may impact risk assessments.
3. Such individuals should be rescreened at the following frequencies:
   1. Annually: For positions with high-security access.
   2. Biannually: For positions with moderate security access.
   3. Every Three Years: For positions with low-risk access.
   4. As Needed: For any incident or change that warrants immediate attention.
4. 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.
   1. Personnel Termination

Departments shall, upon termination of individual employment:

1. Disable information system access within at most 24 hours.
2. Terminate/revoke any authenticators/credentials associated with the individual.
3. Conduct exit interviews that include a discussion of information security policies, nondisclosure agreements, and post-employment obligations
4. Retrieve all security-related information system-related property.
5. Retain access to information and information systems formerly controlled by terminated individual.
6. Notify the [Policy Owner], [Policy Authority], and the individual's supervisor within 24 hours. 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.
7. The entity shall notify terminated individuals of applicable, legally binding post-employment requirements for the protection of information.
8. 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).
9. The entity shall employ automated mechanisms to notify the [Policy Owner], [Policy Authority], Human Resources (HR), and the individual's supervisor upon termination of an individual.
   1. 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 transfer or reassignment actions within 24 hours 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 the [Policy Owner] within 24 hours of transfer. This control applies when reassignments or transfers of individuals are permanent or of such extended durations as to make the actions warranted.
   1. Access Agreements

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

1. Develop and document access agreements for information systems.
2. Review and update the access agreements annually.
3. Ensure that individuals requiring access to information and information systems:
   1. Sign appropriate access agreements prior to being granted access.
   2. Re-sign access agreements to maintain access to information systems when access agreements have been updated or every two years.
   3. Third-Party Personnel Security

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. The [Policy 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 the [Policy Owner] of any personnel transfers or terminations of third-party personnel who possess credentials and/or badges, or who have information system privileges within 24 hours.
4. Monitor provider compliance.
   1. Personnel Sanctions

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. The [Policy Owner] shall:

1. Employ a formal sanction process for individuals failing to comply with established information security policies and procedures
2. Notify [Policy Owner] within 24 hours when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

# 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 [Policy 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 [Policy Authority] will review and discuss these requests with the department.

# 7.0 Definitions of Key Terms

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Information Systems | Any combination of hardware, software, data, and personnel that processes, stores, or transmits information, including but not limited to computers, servers, networks, and applications. |
| Users | Individuals or entities, including employees, contractors, and third-party vendors, who access or interact with the organization’s information systems and data. |
|  |  |

# 8.0 Contact Information

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

[Policy Owner’s Contact Info]

[Organization Address]

# 9.0 Review and Revision

This policy should be reviewed at least annually to keep pace with evolving regulations, threat landscapes, and organizational changes. However, more frequent reviews may be necessary following regulatory updates, cybersecurity incidents, significant technology changes, organizational shifts, or compliance audits. This policy should be revised based on these reviews and those revisions noted below.

|  |  |  |
| --- | --- | --- |
| **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)