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

# 1.0 Purpose and Benefits

The purpose of this risk assessment policy is to establish a systematic approach for identifying, evaluating, and managing risks associated with the organization’s information technology (IT) systems and assets. By requiring regular assessments of vulnerabilities and potential threats, the policy aims to ensure compliance with established IT security standards and protocols. This proactive framework not only safeguards sensitive information from unauthorized access and breaches but also enhances the overall cybersecurity posture of the organization. Through thorough risk assessments, the organization can prioritize resources effectively, address vulnerabilities in a timely manner, and implement appropriate controls to mitigate identified risks.

Implementing this risk assessment policy offers numerous benefits, including enhanced protection of the organization’s critical information assets, improved compliance with regulatory requirements, and increased stakeholder confidence in the organization’s security measures. By systematically identifying and analyzing risks, the organization can make informed decisions about resource allocation and security investments, ultimately reducing the likelihood of security incidents and their potential impact. Furthermore, the policy fosters a culture of security awareness among employees, contractors, and third-party vendors, emphasizing their role in safeguarding organizational data. Regular updates and dissemination of risk assessment results promote transparency and facilitate collaboration among stakeholders, reinforcing the organization’s commitment to maintaining a secure information environment.

# 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 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.

* 1. Security Categorization

The [Policy Owner] shall:

1. Apply proper security controls to data categorized as confidential by system owners, including protected health information (PHI) and personally identifiable information (PII), in accordance with applicable federal and state laws, directives, policies, regulations, standards, and guidance.
2. Document the security controls (including supporting rationale) in the security plan for the information system.
   1. Risk Assessment

The [Policy Owner] shall:

1. Conduct (or have conducted by a qualified third-party) an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits.
2. Document risk assessment results in annual IT Risk Assessment.
3. Review risk assessment results quarterly.
4. Disseminate risk assessment results to stakeholders.
5. Update the risk assessment quarterly or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.
   1. Vulnerability Scanning

The [Policy Owner] shall:

1. Conduct (or have conducted by a qualified third-party) a comprehensive assessment of vulnerabilities within the information system, including the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the information it processes, stores, or transmits. This assessment shall include:
   1. Identification of all system components, applications, and data that are subject to potential vulnerabilities.
   2. Evaluation of existing security controls specifically related to vulnerability management and their effectiveness in mitigating risks.
   3. Analysis of known vulnerabilities, including those identified in security advisories and databases (e.g., CVE, NVD), that may affect the information system.
   4. Assessment of the potential impact of identified vulnerabilities on organizational operations and data integrity, including the potential for exploitation and associated consequences.
   5. Review of the organization’s current vulnerability scanning practices, including frequency, tools used, and scope, to ensure alignment with industry best practices and compliance requirements.
2. Employ vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
   1. Enumerating platforms, software flaws, and improper configurations.
   2. Formatting checklists and test procedures.
   3. Measuring vulnerability impact.
3. Analyze vulnerability scan reports and results from security control assessments.
4. Remediate legitimate vulnerabilities within one month in accordance with an organizational assessment of risk.
5. Share information obtained from the vulnerability scanning process and security control assessments with the [Authority] to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).
6. Employ vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned.
7. Update the information system vulnerabilities scanned monthly, prior to a new scan, or when new vulnerabilities are identified and reported.
8. Ensure that information systems implement privileged access authorization to all systems for selected vulnerability scanning.

# 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** |
| 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) SP 800-30, Guide for Conducting Risk Assessments](https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final" \t "_blank)

[National Institute of Standards and Technology (NIST) SP 800-39, Managing Information Security Risk](https://csrc.nist.gov/publications/detail/sp/800-39/final#:~:text=The%20purpose%20of%20Special%20Publication,the%20Nation%20resulting%20from%20the)

[National Institute of Standards and Technology (NIST) SP 800-115, Technical Guide to Information Security Testing and Assessment](https://csrc.nist.gov/pubs/sp/800/115/final)

[National Institute of Standards and Technology (NIST) SP 800-137; Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations](https://csrc.nist.gov/pubs/sp/800/137/final)