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

# 1.0 Purpose and Benefits

# To ensure that Information Technology (IT) performs risk assessments in compliance with IT security policies, standards, and procedures.

# 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.

# 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.

### Security Categorization

* 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.

### Risk Assessment

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.

### Vulnerability Scanning

1. Scan for vulnerabilities in the information system and hosted applications quarterly and/or randomly in accordance with [entity defined process] and when new vulnerabilities potentially affecting the system/applications are identified and reported.
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 |
|  |  |

# 8.0 Contact Information

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

[Organization Address & Policy Owner’s Contact Info]98.0 Revision History

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

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

# 10.0 Related Documents

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

[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)