SecOps® Solution

Risk Assessment Policy

Free Use Disclaimer: *This policy may be utilized entirely or in part by your organization without restriction. There is no need for prior authorization. Please email hello@secopsolution.com if you would like to contribute a new or updated version of this one.*

1. Overview

A risk assessment policy is a set of guidelines and procedures that organizations use to evaluate potential risks and vulnerabilities associated with their operations, systems, or projects.

2. Purpose

To provide Infosec the authority to conduct recurring information security risk assessments (RAs) in order to identify any areas of vulnerability and to start the necessary remediation.

3. Scope

Every entity within **<Company Name>** or an outside business that has a Third Party Agreement in place with **<Company Name>** may be the subject of risk assessments. Any information system, such as applications, servers, and networks, as well as any process or technique used to manage and/or maintain these systems, is subject to RAs.

4. Policy

Infosec and the department in charge of the system area under evaluation are jointly responsible for the execution, creation, and implementation of remediation initiatives. Any RA being undertaken on systems for which employees are held accountable is anticipated to get full employee cooperation. Also, workers are expected to collaborate on the creation of a remediation plan with the Infosec Risk Assessment Team.

4.1 Security Categorization

IT Department shall:

- 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.

- Document the security controls (including supporting rationale) in the security plan for the information system.

4.2 Risk Assessment

IT Department shall:

- Conduct (or have conducted by a qualified third party) an assessment of risk, including the likelihood and magnitude of the harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits.
- Document risk assessment results in the annual IT Risk Assessment.
- Review risk assessment results quarterly.
- Disseminate risk assessment results to stakeholders.
- 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.

4.3 Vulnerability Scanning

IT Department shall:

- 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.
- 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.
- Analyze vulnerability scan reports and results from security control assessments.
- Remediate legitimate vulnerabilities within one month in accordance with an organizational assessment of risk.

- Share information obtained from the vulnerability scanning process and security control assessments with the Chief Information Officer to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).
- Employ vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned.
- Update the information system vulnerabilities scanned monthly, prior to a new scan, or when new vulnerabilities are identified and reported.
- Ensure that information systems implement privileged access authorization to all systems for selected vulnerability scanning.

For additional information, go to the Risk Assessment Process.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec Team will verify compliance with this policy through various methods, including but not limited to, business tool reports, internal and external audits, and inspection, and will provide feedback to the policy owner and appropriate business unit manager.

5.2 Exceptions

Any exception to the policy must be approved by Remote Access Services and the Infosec Team in advance.

5.3 Non-Compliance

An employee who has violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies, and Processes

- Risk Assessment Process
- Third Party Agreement

7. Revision History

Version	Date	Description
1.0	07-03-2023	Initial Policy