# Security Assessment Policy

To use this template, simply replace the text in dark grey with information customized to your organization. When complete, delete all introductory or example text and convert all remaining text to black prior to distribution.

# Purpose

Describe the factors or circumstances that mandate the existence of the policy. Also state the policy’s basic objectives and what the policy is meant to achieve.

The quality and integrity of [Company Name’s] security assessment is focused on determining the degree to which information system security controls are correctly implemented, whether they are operating as intended, and whether they are producing the desired level of security. Vulnerability assessment is focused on determining the weaknesses inherent in the information systems that could be exploited, leading to information system breach. Without security and vulnerability assessments, the potential exists that information systems may not be as secure as intended or desired.

# Scope

Define to whom and to what systems this policy applies. List the employees required to comply, or simply indicate “all” if all must comply. Also indicate any exclusions or exceptions, i.e. those people, elements, or situations that are not covered by this policy or where special consideration may be made.

This Security Assessment Policy applies to all information systems and information system components of [Company Name]. Specifically, it includes:

* Mainframes, servers, and other devices that provide centralized computing capabilities.
* SAN, NAS, and other devices that provide centralized storage capabilities.
* Desktops, laptops, and other devices that provide distributed computing capabilities.
* Routers, switches, and other devices that provide network capabilities.
* Firewalls, IDP sensors, and other devices that provide dedicated security capabilities.

# Definitions

Define any key terms, acronyms, or concepts that will be used in the policy. A standard glossary approach is sufficient.

# Governing Laws & Regulations

If applicable, list any laws or regulations that govern the policy or with which the policy must comply. Confirm with the legal department that the list is full and accurate. If there are no pertinent governing laws or regulations, delete this section.

# Policy Statements

Describe the rules that comprise the policy. This typically takes the form of a series of short prescriptive and proscriptive statements. Sub-dividing this section into sub-sections may be required depending on the length or complexity of the policy.

1. Security assessments will be performed against all information systems on an [indicate frequency – suggest annual] basis. Vulnerability assessments will be performed against all information systems on a [indicate frequency – suggest quarterly] basis.
2. While both security and vulnerability assessments are to be performed by internal staff on an on-going basis, third parties will be retained every [indicate frequency – suggest third] assessment to ensure appropriate levels of coverage and oversight.

**Relevant Procedures**

Consider creating formal procedure documents that reinforce and support the policy statements above. Note, it is best practice to house policies and procedures in separate documents to keep the content focused and reduce the number of times the policy must be reapproved by senior management.

Perform security and vulnerability assessments against enterprise networks and information systems:

* + - * + Develop an assessment plan:

*Determine the scope of assessments to be performed.*

*Establish a prioritized assessment schedule.*

*Identify and gather required skills and tools.*

*Create an assessment implementation plan.*

* + - * + Execute the assessment plan:

*Review system documentation, including system configuration documents and system log files, to determine expected security configuration and capabilities of the system.*

*Identify and analyze the target system through investigative techniques that include network foot-printing, port and service scanning, and vulnerability assessment.*

*Validate vulnerabilities that may be discovered through validating techniques that include penetration testing, password cracking, and social engineering.*

* + - * + Analyze assessment data and report on findings:

*Review validated assessment findings to determine the risk and cost impact on the organization.*

*Create a final report outlining the findings of the assessment.*

# Non-Compliance

Clearly describe consequences (legal and/or disciplinary) for employee non-compliance with the policy. It may be pertinent to describe the escalation process for repeated non-compliance.

Violations of this policy will be treated like other allegations of wrongdoing at [Company Name]. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable [Company Name] policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements.