# IT Security Risk Strategy 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.

|  |  |
| --- | --- |
| **Policy Owner** | Name the person/group responsible for this policy’s management. |
| **Policy Approver(s)** | Name the person/group responsible for implementation approval of this policy. |
| **Related Policies** | Name other related enterprise policies both within or external to this manual. |
| **Related Procedures** | Name other related enterprise procedures both within or external to this manual. |
| **Storage Location** | Describe physical or digital location of copies of this policy. |
| **Effective Date** | List the date that this policy went into effect. |
| **Next Review Date** | List the date that this policy must undergo review and update. |

# 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 purpose of this policy is to ensure adequate processes and controls are in place to mitigate risks and measure progress related to security performance.

# 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 IT Security Risk Strategy Policy applies to all business processes and data, information systems and components, personnel, and physical areas of [Insert Company’s Name].

# Definitions

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

# Governing Laws, Regulations, and Standards

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.

|  |  |
| --- | --- |
| **Guidance** | **Section** |
| NIST SP 800-30 | Risk Assessment (3.1 – 3.9), Mitigation (4.1 – 4.6) |
| NIST SP 800-53 v4 | PM-9, CP-2, RA-3 |

# 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.

**Risk Assessment and Mitigation:**

* Security risk tolerance level should be defined, documented, and communicated across [Insert Company’s Name].
* Security risk assessment criteria should be defined in order to produce consistent assessment results.
* Risk assessments will be performed on all information systems that house or access [Insert Company’s Name] controlled information. These assessments will address unauthorized access, use, disclosure, disruption, modification, and/or destruction of information or the information system itself. Further, the assessments shall identify known potential threats, the likelihood of their occurrence, and the magnitude of the impact of those threats should they occur.
* Risk assessments shall be performed upon initial acquisition of an information system (in the event that the information system is owned/operated by [Insert Company’s Name]) or prior to initial establishment of service agreements (in the event that the information system is owned/operated by a third party on behalf of [Insert Company’s Name]). Further, the risk assessment shall be reviewed and, where required, updated after *[indicate interval – suggest three years]* or whenever a significant change is made to the information system, whichever comes first.
* Results of risk assessments will be disseminated to appropriate parties.

**Third-Party Risk Management:**

* + Prior to choosing a third party, a proper risk assessment must be conducted on the third party to ensure reputation, security practices, etc. are clearly made evident and work within [Insert Company’s Name]’s risk tolerance.
	+ Third parties must provide documentation around their own risk management procedures, staffing requirements, recordkeeping, and security processes.
	+ 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.

**Security Performance and Metrics:**

* + [Insert Company’s Name] will determine what needs to be monitored and measured to demonstrate effectiveness of security and overall risk management processes (e.g. incident reporting, and decrease in overall incidents).

**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.

# 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.