**Risk Management Policy**

# ***Version Control Table***

| Version | Date | Author | Description |
| --- | --- | --- | --- |
| 1.0 |  |  |  |
| 1.0 |  |  |  |
| 1.0 |  |  |  |
| **1.0** |  |  |  |
|  |  |  |  |

| **Date of Next Revision** |  |
| --- | --- |

This policy will be reviewed for continued completeness, relevance, and accuracy within 1 year of being granted “final” status, and at yearly intervals thereafter.

The version control table will show the published update date and provide a thumbnail of the major change. CAUTION: the thumbnail is not intended to summarise the change and not a substitute for reading the full text.

# ***Table of Contents***

[**Version Control Table**](#_1t3h5sf) **2**

[**Table of Contents**](#_4d34og8) **3**

[**Purpose**](#_7s6z329mfess) **4**

[**Scope**](https://docs.google.com/document/d/1yZrppDWiQyHjI0hJotHztX5pVZHvmA2cCRsdZC8-W_E/edit#heading=h.98gh1c20134h)[**4**](https://docs.google.com/document/d/1yZrppDWiQyHjI0hJotHztX5pVZHvmA2cCRsdZC8-W_E/edit#heading=h.98gh1c20134h)

[**Disaster Recovery Plan**](https://docs.google.com/document/d/1yZrppDWiQyHjI0hJotHztX5pVZHvmA2cCRsdZC8-W_E/edit#heading=h.htj2nywx40qj)[**4**](https://docs.google.com/document/d/1yZrppDWiQyHjI0hJotHztX5pVZHvmA2cCRsdZC8-W_E/edit#heading=h.htj2nywx40qj)

[**Disaster Recovery Team**](https://docs.google.com/document/d/1yZrppDWiQyHjI0hJotHztX5pVZHvmA2cCRsdZC8-W_E/edit#heading=h.w74atipusb2a)[**4**](https://docs.google.com/document/d/1yZrppDWiQyHjI0hJotHztX5pVZHvmA2cCRsdZC8-W_E/edit#heading=h.w74atipusb2a)

[**Critical Systems and Services**](https://docs.google.com/document/d/1yZrppDWiQyHjI0hJotHztX5pVZHvmA2cCRsdZC8-W_E/edit#heading=h.g5allkydhzj0)[**4**](https://docs.google.com/document/d/1yZrppDWiQyHjI0hJotHztX5pVZHvmA2cCRsdZC8-W_E/edit#heading=h.g5allkydhzj0)

[**Disaster Recovery Action Plan**](https://docs.google.com/document/d/1yZrppDWiQyHjI0hJotHztX5pVZHvmA2cCRsdZC8-W_E/edit#heading=h.81iiqndrfmol)[**5**](https://docs.google.com/document/d/1yZrppDWiQyHjI0hJotHztX5pVZHvmA2cCRsdZC8-W_E/edit#heading=h.81iiqndrfmol)

[**Notification Phase**](https://docs.google.com/document/d/1yZrppDWiQyHjI0hJotHztX5pVZHvmA2cCRsdZC8-W_E/edit#heading=h.uxx5r2qmghfm)[**5**](https://docs.google.com/document/d/1yZrppDWiQyHjI0hJotHztX5pVZHvmA2cCRsdZC8-W_E/edit#heading=h.uxx5r2qmghfm)

[**Recovery Phase**](https://docs.google.com/document/d/1yZrppDWiQyHjI0hJotHztX5pVZHvmA2cCRsdZC8-W_E/edit#heading=h.7qthrmi4ht8n)[**5**](https://docs.google.com/document/d/1yZrppDWiQyHjI0hJotHztX5pVZHvmA2cCRsdZC8-W_E/edit#heading=h.7qthrmi4ht8n)

[**Reconstitution Phase**](https://docs.google.com/document/d/1yZrppDWiQyHjI0hJotHztX5pVZHvmA2cCRsdZC8-W_E/edit#heading=h.atx586aeo87r)[**5**](https://docs.google.com/document/d/1yZrppDWiQyHjI0hJotHztX5pVZHvmA2cCRsdZC8-W_E/edit#heading=h.atx586aeo87r)

[**Forensics Phase**](https://docs.google.com/document/d/1yZrppDWiQyHjI0hJotHztX5pVZHvmA2cCRsdZC8-W_E/edit#heading=h.6rbvm7pzwssw)[**5**](https://docs.google.com/document/d/1yZrppDWiQyHjI0hJotHztX5pVZHvmA2cCRsdZC8-W_E/edit#heading=h.6rbvm7pzwssw)

[**Retrospective Phase**](https://docs.google.com/document/d/1yZrppDWiQyHjI0hJotHztX5pVZHvmA2cCRsdZC8-W_E/edit#heading=h.hmv4dmb32xjz)[**6**](https://docs.google.com/document/d/1yZrppDWiQyHjI0hJotHztX5pVZHvmA2cCRsdZC8-W_E/edit#heading=h.hmv4dmb32xjz)

[**After Disaster Test Phase**](https://docs.google.com/document/d/1yZrppDWiQyHjI0hJotHztX5pVZHvmA2cCRsdZC8-W_E/edit#heading=h.6snfqhlw7dm4)[**6**](https://docs.google.com/document/d/1yZrppDWiQyHjI0hJotHztX5pVZHvmA2cCRsdZC8-W_E/edit#heading=h.6snfqhlw7dm4)

[**Disaster Recovery testing**](https://docs.google.com/document/d/1yZrppDWiQyHjI0hJotHztX5pVZHvmA2cCRsdZC8-W_E/edit#heading=h.grmx9find4xd)[**6**](https://docs.google.com/document/d/1yZrppDWiQyHjI0hJotHztX5pVZHvmA2cCRsdZC8-W_E/edit#heading=h.grmx9find4xd)

[**Change, Review, and Update**](https://docs.google.com/document/d/1yZrppDWiQyHjI0hJotHztX5pVZHvmA2cCRsdZC8-W_E/edit#heading=h.w1o88vxspwq8)[**6**](https://docs.google.com/document/d/1yZrppDWiQyHjI0hJotHztX5pVZHvmA2cCRsdZC8-W_E/edit#heading=h.w1o88vxspwq8)

[**Disciplinary Action**](https://docs.google.com/document/d/1yZrppDWiQyHjI0hJotHztX5pVZHvmA2cCRsdZC8-W_E/edit#heading=h.nubzoem94o3x)[**7**](https://docs.google.com/document/d/1yZrppDWiQyHjI0hJotHztX5pVZHvmA2cCRsdZC8-W_E/edit#heading=h.nubzoem94o3x)

[**Responsibility**](https://docs.google.com/document/d/1yZrppDWiQyHjI0hJotHztX5pVZHvmA2cCRsdZC8-W_E/edit#heading=h.hbuyrp1djidk)[**7**](https://docs.google.com/document/d/1yZrppDWiQyHjI0hJotHztX5pVZHvmA2cCRsdZC8-W_E/edit#heading=h.hbuyrp1djidk)

[**Related documents**](https://docs.google.com/document/d/1yZrppDWiQyHjI0hJotHztX5pVZHvmA2cCRsdZC8-W_E/edit#heading=h.cot3aomf1czt)[**7**](https://docs.google.com/document/d/1yZrppDWiQyHjI0hJotHztX5pVZHvmA2cCRsdZC8-W_E/edit#heading=h.cot3aomf1czt)

# 

# **Purpose**

The purpose of this document is to define the *[Company]’s* information security risk management process – which includes the risk assessment and the risk treatment processes and to provide the requirements to ensure that security risks are continually recognized, reviewed, and mitigated, as appropriate.

# **Principles**

*[Company]* believes that effective risk management involves:

* A commitment to the security of *[Company]* infrastructure and services from senior management;
* The involvement, cooperation, and insight of all *[Company]* staff;
* A commitment to initiating risk assessments, starting with discovery and identification of risks;
* A commitment to the thorough analysis of identified risks;
* A commitment to a strategy for the treatment of identified risks;
* A commitment to communicate all identified risks to the company;
* A commitment to encouraging the reporting of risks and threat vectors from all *[Company]*.

# **Scope**

This Risk Management Policy applies to all *[Company]’s* systems and data, owned by *[Company]* or operated on behalf of *[Company]*.

Vendor-related risks are covered under Supply Chain and Business Partner Policy, which includes a thorough risk assessment targeted at a vendor's security, business practices, legal commitments, and insurance postures.

# **Policy**

* *[Company]* risk assessment methodology is based on [**NIST Special Publication 800-30 Revision 1 - Guide for Conducting Risk Assessments**](https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf), and [**ISO/IEC 27005 "Information technology — Security techniques — Information security risk management"**](https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-3:v1:en).
* The assigned person shall communicate the risk assessment results obtained to the risk owners, and reach an agreement on the results and further risk mitigation.
* The risk management methodology will be updated as required due to the results of audits and incidents.
* This risk assessment policy specifies how and when risk assessments will be done and who will be responsible for conducting risk assessments and implementing solutions to address any risk assessment findings.
* It is the responsibility of all *[Company]* staff to identify, analyze, evaluate, monitor, and communicate risks associated with any activity, technology, function, or process within their relevant scope of responsibility and authority.
* *[Company]* performs at least one risk assessment every year, or when the critical changes occur using qualified internal staff and/or external third parties who have experience performing risk assessments.
* A risk assessment should be done or reviewed on critical systems and applications no less than every two years.
* Risk assessments may be used to assess all risks to the organization.
* The result of the risk assessment is to have a report with a risk action plan. The action plan will be a plan for implementing additional controls and solutions to mitigate or manage the risk by appropriate risk owners.
* The risk assessment process and methodology will be updated as required due to the results of audits and incidents.
* All identified vulnerabilities will be assessed for impact and criticality. Vulnerabilities must be remediated as soon as possible.

## **Third-Party Risks**

* *[Company]* identifies all third parties that access our customer data.
* *[Company]* acknowledges the risks associated with vendor providers and ranges them according to the criticality of the third party accessing the customer. *[Company]* commits to addressing the security of the third-party vendors regularly.

## **Annual Review**

* *[Company]* will conduct an annual, formal Risk Assessment that identifies current and possible threats and vulnerabilities.
* *[Company]* is reviewing its policies, procedures, standards, and guidelines in accordance with the updated Risk Assessment and making any applicable modifications to counter evolving threats.

# **Risk Assessment Plan**

Based on *AICPA Cybersecurity Risk Management Framework*.

* Management defines the scope of risk assessment.
* The proper time and method of communicating the selected risk treatment options to the affected IT, and business management should be included.
* Evaluate the system - Determine if the system is critical to the organization's business processes and determine the data classification and security needs of the data on the system, considering security needs.
* List the threats - List possible threat sources such as an exploitation of a vulnerability.
* Identify vulnerabilities.
* Evaluate potential security controls already in place to assess if they adequately address the risk.
* Identify the probability of exploitation. Additional security controls may need to be in place before the probability of exploitation is lowered.
* Quantify damage (impact) - Categorize the damage.
* Determine risk level - Use likelihood times impact to quantify the amount of risk.
* Evaluate and recommend controls to reduce or eliminate risk - Identify existing controls and those that may further reduce probabilities or mitigate specific vulnerabilities. List specific threats and vulnerabilities for the system to help identify mitigating controls.
* Create the risk assessment report.
* Communicate the selected risk treatment options to the affected IT and business management and staff.
* Take recommended risk mitigation actions. Record such actions as changes per the *[Company]’s* Change Management program.
* Monitor the effectiveness of the risk mitigation actions and document the results.

## **Risk Identification and Assessment**

* These risks should be taken into consideration:
  + Risk highlighted in the results of vulnerability scans or penetration testings
  + Risks communicated by any of *[Company]* employees
  + Risks discovered during the processing of business partner’s questionnaires
  + Risks related to the critical assets of the company
* IT Manager or the outsourced professional evaluates potential security controls already in place to assess if they adequately address the identified risks. This also includes identifying the appropriate control owners for each control objective.
* Identification of the probability of exploitation. Additional security controls may need to be in place before the probability of exploitation is lowered.
* Qualify damage (impact) - Responsible person categorizes the damage by the level of threat impact. This will help when looking at the cost of controls to reduce the risk.
* Determine risk level - Responsible person uses probability times impact to qualify the amount of risk.

## **Risk Acceptance**

* When the probability of threat materialization times maximum damage amount is less than $1000 annually, the risk is acceptable. For higher amounts, on a yearly basis, acceptance of the risk will depend on the cost of implementing measures to reduce the risk. If the risk cannot be reduced and the amount per year is greater than $50,000, the risk should be transferred by purchasing insurance.

## **Risk Mitigation**

* Costs of implementing each control are considered and compared to the benefits, of implementing each control.
* Cost and benefit analyses are done to evaluate proposed controls versus risks. When the controls are evaluated, the benefits, costs, and cost savings of applying the controls both individually and in combination should be determined. Performance measures for determining the effectiveness of the new controls are created.
* Risks should be ranked, and controls are selected, and a plan created to implement the controls. Responsibilities for implementing the controls are determined and communicated. Budgeting and schedules are set and the expected outcomes from mitigating the risks with the controls are documented. Residual risk after full implementation is considered.
* Decisions regarding residual risk are made. Specifically, whether to accept the risk, transfer the risk, or take other action, including adding additional controls.
* Safeguard options for addressing high-risk scenarios must be considered and utilized appropriately while the extent of risk reduction and benefits are considered. Cost and benefit analyses are done to evaluate safeguard options.
* Suppose the cost of safeguard options or recommended risk controls is greater than the available budget. In that case, the options and controls are prioritized to reduce as much risk as possible within the budget.
* When the risk assessment report is completed, results shall be communicated to the affected IT and business management and staff.

## **Measurements**

**Risk = Threat Probability x Magnitude of Impact**

*[incert the table with this info]*

# **Disciplinary Action**

Employees who violate this policy may face disciplinary consequences in proportion to their violation. Our management will determine how severe an employee’s offense is and take the appropriate action.

# **Responsibility**

The Legal Counsel is responsible for ensuring this policy is followed.

This policy shall be reviewed yearly or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

# Reference

* *[SOC 2 or ISO 27001 controls]*

# **Related Documents**

* Supply Chain and Business Partner Policy