©(ORGANISATION NAME)

RISK ASSESSMENT POLICY

Subject: Risk Assessment Policy		Author: MuVio Solutions Ltd
Document Type: Policy (Internal)	Page: 1 of 20	Authorised by:
Effective Date: June 2024	Version 1.0	Next Review:

Author	Signature	Date
Muvio Solutions Ltd (Consultant Designation)		

Revision History:

Version	Date	Change Number	Summary of Changes
1.0	April, 2024		

Distribution:

Name	Title

Approved By:

Name	Signature	Date
Name (Designation)		
Name (Designation)		
Name (Designation)		
Name (Designation)		

Document Ownership

Information Security

Document Control

The validity of this document is limited to the use of the policy as a guideline for Information Security Organisation-wide. In the event that the adopted policy framework changes, the document will have to be reviewed and the document owner must assess this

document for relevancy at that point. This document will be reviewed at least annually and updated accordingly to reflect changes to business objectives or the risk environment.

Document Control

The Document Owner controls the distribution of this document. The distribution is as follows:

- Chief Information Security Officer
- Chief Information Officer
- Chief Risk Officer
- Chief Audit Executive
- Chief Compliance Officer
- Head, Human Resources

Notice and Warning

CONTENTS

1.0 OVERVIEW

The effective management of information security has been and remains a paramount priority for the Organisation to manage risk exposures and safeguard its reputation in the marketplace. This policy outlines the framework for the Organisation's security risk assessment processes. It provides an objective, technical evaluation of the likelihood of unacceptable impacts to the Organisation's information and information assets. The objective is to establish a well-defined process for identifying, analysing, evaluating, and mitigating risks associated with our Organisation and with the third-party partnerships to ensure adherence to the Organisation's security and compliance standards, thereby safeguarding information assets and preserving the integrity of business processes.

1.1 PURPOSE

The purpose of this policy is to describe how the information security risk assessment is managed. This includes the severity of the risk and how it is reported, including the identification of key information assets and their associated risk.

The risk assessment and treatment actions are reviewed on a minimum of an annual basis. The status of risks and, where appropriate, treatment activities will be maintained by the Information Security and Operational Risk Management departments.

1.2 OBJECTIVES

- To identify, analyse, evaluate, and proffer treatment for identified information security risks.
- To ensure that residual risk falls within the risk acceptance criteria.
- To record, review and update the information security risk assessment findings.

1.3 SCOPE

This policy is applicable to all employees of the Organisation, as well as any third-party entities engaged in the Organisation's business operations or granted access to the Organisation's confidential or sensitive information. Such third-party relationships include vendors, service providers, contractors, and any other external parties.

2. POLICY DETAILS

2.1 CRITERIA FOR PERFORMING INFORMATION SECURITY RISK ASSESSMENTS

The following are the circumstances in which a risk assessment should be performed:

▪ A comprehensive risk assessment covering all information assets as part of the initial implementation of the Information Security Framework.

▪ The organisation's Risk Appetite shall be defined, reviewed and approved by the Board of Directors.

▪ Updates to the comprehensive risk assessment as part of the management review process.

▪ As part of projects that involve significant change to the Organisation or the Information Security Framework.

▪ On major change affecting the Organisation which may invalidate the conclusions from previous risk assessments conducted.

The risk assessment would be conducted in two ways:

Asset-based Risk Assessment: Asset-based risk assessments focus on the risks facing individual assets to control them.

Scenario-based Risk Assessment: Scenario-based risk assessments look at the risks facing the Organisation's information more generally and assess the necessary controls based on those risks.

The following steps are followed during a Risk Assessment process:

1. Identify the Name of the Asset/Service.

2. Identify the Owner of the Asset/Service.

3. Specific type of Asset/Service.

4. The security classification of the information held by the asset.

5. Specific identification of the assets.

6. The physical or logical location of the asset

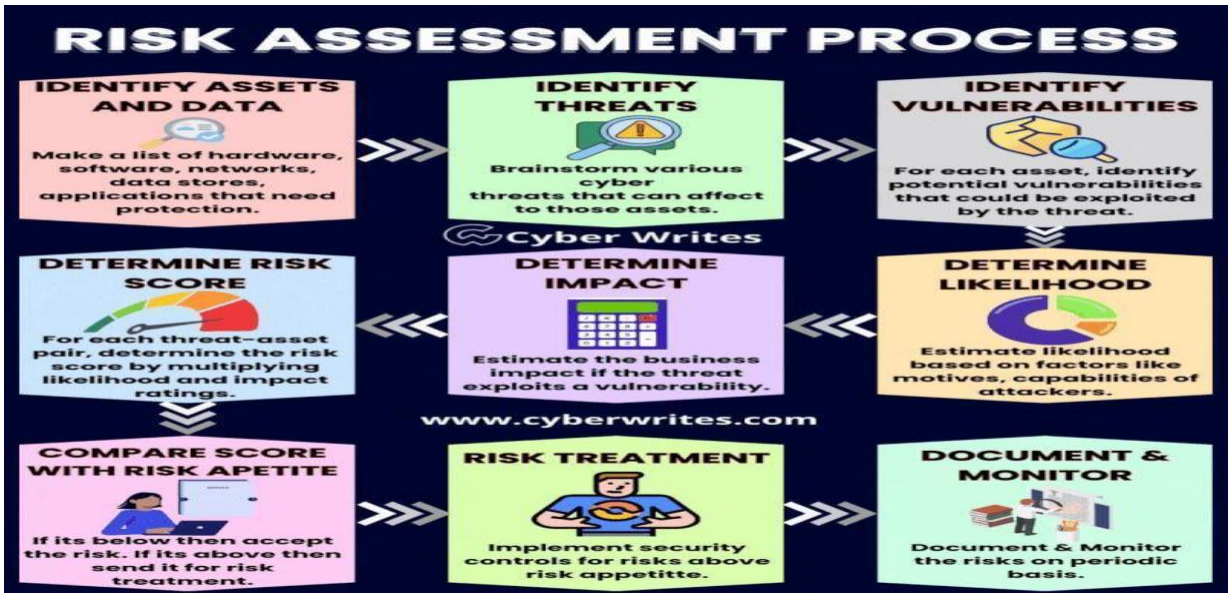
7. The appropriate legal, regulatory, and contractual obligations for each asset.

8. The risk to the asset is then assigned a score and calculated.

9. The treatment plan is identified as to how the risk of compromise of the asset/service is to be implemented.

10. The Risk Assessment will be conducted on an annual basis, or when there is a significant change or incident in the Organisation.

Fig 1 below shows risk assessments process:



Risk Acceptance Criteria:

The criteria for acceptance of risk within Organisation shall include:

- When the risk value is lower than the acceptance threshold, the risk shall be accepted.
- When the risk value is higher than the threshold, the risk shall be treated and if after treatment, the likelihood of the occurrence can be reduced or may remain the same if controls implemented are not robust enough as certified by Top Management.

2.1.1 DEFINING AND SCORING RISKS

The impact to the loss of confidentiality, integrity, availability (CIA) is assessed as it relates to the defined asset/service. For each asset/service you have defined, you need to assign risks or scenarios.

The impact to the loss of confidentiality, integrity, availability (CIA) is:

- Assessed and defined in terms of the applicability and compromise it represents (to confidentiality, integrity and/or availability)
- The impact it could result in and the likelihood of the risk coming to pass for individual Assets.

2.1.2 RISK ASSESSMENT SCALES

Attribute	Score	Description
Confidentiality	Low	Describes all information, information processing facilities, and system resources that are accessible to anyone within the organisation, e.g., the information on our public website. The impact of unauthorised disclosure on the organisation's operations would be negligible or inconsequential.
	Medium	Describes all information, information processing facilities, and system resources that should only be accessed by organisational staff without restrictions, but not by anyone else. The impact of unauthorised disclosure on the organisation's operations would be minor or moderate.
	High	Describes all information, information processing facilities, and system resources that should only be accessed by organisational staff if explicitly authorised to do so. The impact of unauthorised disclosure on the organisation's operations would be significant, and such incidents should be avoided.
	Very High	Describes all information, information processing facilities, and system resources that require explicit high-level authorisation for access. The impact of unauthorised disclosure on the organisation's operations would be severe or catastrophic, and such incidents must be avoided under all circumstances.

Integrity	Low	Describes all information, information processing facilities and system resources for which the need for integrity is of little or no consequence. The impact of unauthorised modification, corruption, or loss of such asset on Organisation operations would be negligible/insignificant
	Medium	Describes all information, information processing facilities and system resources for which the need for information integrity is of minor importance but should generally be maintained. The impact of unauthorised modification, corruption, or loss on Organisation operations would be minor/ moderate
	High	Describes all information, information processing facilities and system resources for which the need for information integrity is important and should be well controlled. The impact of unauthorised modification, corruption, or loss on Organisation operations would be considerable and should be protected against.
	Very High	Describes all information, information processing facilities and system resources for which the need for information integrity is very important and should be maintained under all circumstances. The impact of unauthorised modification, corruption, or loss on Organisation operations, assets and individuals would be severe and should be strongly protected against.

Availability	Low	Describes all information, information processing facilities and system resources where availability is not critical, and it is sufficient for this asset to be available within 24 hours. The impact of a disruption of access to or use of such asset on Organisation operations would be negligible
	Medium	Describes all information, information processing facilities and system resources which should be available within a workday i.e. less than 8 hours. The impact of a disruption of access to or use of such asset on Organisation operations would be minor/moderate
	High	Describes all information, information processing facilities and system resources which should be available within a few hours. The impact of a disruption of access to or use of such asset on Organisation operations would be significant
	Very High	Describes all information, information processing facilities and system resources which should be available immediately on demand, and unavailability of the asset would cause a serious impact to Organisation business. The impact of a disruption of access to or use of such asset on Organisation operations would be severe/catastrophic.

Asset Value

Availability	Integrity	Low				Medium				High				Very High			
	Confidentiality	L	M	H	VH	L	M	H	VH	L	M	H	VH	L	M	H	VH
	Low	1	2	3	4	2	4	6	8	3	6	9	12	4	8	12	16
	Medium	2	4	6	8	4	8	12	16	6	12	18	24	8	16	24	32
	High	3	6	9	12	6	12	18	24	9	18	27	36	12	24	36	48
	Very High	4	8	12	16	8	16	24	32	12	24	36	48	16	32	48	64

Asset Value=(Confidentiality) x (Integrity) x (Availability)

Level	Low	Medium	High	Very High
Score	**1**	**2**	**3**	**4**
Value	1 to 12	13 to 18	19 to 36	37 to 64

Threat Assessment Scale

The following 4-point valuation scale is used for scoring identified threats in terms of the likelihood of successfully exploiting identified vulnerabilities.

Threat Level Definitions	
Level	Description
Low	This describes a threat that is unlikely to occur, or the likelihood of successfully exploiting an identified vulnerability is improbable, i.e., less than once per year.
Medium	This describes a threat that is possible but only moderately probable, i.e., the likelihood of successfully exploiting an identified vulnerability is about once per year.
High	This describes a threat that is probable, or the likelihood of successfully exploiting an identified vulnerability is between 2–3 times per year.
Very High	This describes a threat that is highly probable, or the likelihood of successfully exploiting an identified vulnerability is more than 3 times per year.

Vulnerability Assessment Scale

The following 4-point valuation scale is used for scoring an identified vulnerability in terms of the likelihood of its exploitation by an identified threat.

Vulnerability Level Definitions	
Level	Description
Low	This describes a trivial or minor vulnerability, or one for which the likelihood of exploitation by an identified threat source is remote or improbable, i.e., less than once per year.
Medium	This describes a moderate vulnerability for which the likelihood of exploitation by an identified threat source is about once per year.
High	This describes a serious vulnerability for which the likelihood of exploitation by an identified threat source is about 2–3 times per year.
Very High	This describes a severe vulnerability for which the likelihood of exploitation by an identified threat source is more than 3 times per year.

Likelihood of Exposure Matrix

This matrix denotes the combined effect of each threat/vulnerability pair in terms of the likelihood of both factors coming together to expose an asset to loss or damage i.e. (Threat x Vulnerability). A total of 4 assessment scores are defined as depicted below.

EXPOSURE/PROBABILITY OF OCCURRENCE MATRIX					
VULNERABILITY	**Very High (4)**	**4**	**8**	**12**	**16**
	High (3)	**3**	**6**	**9**	**12**
	Medium (2)	**2**	**4**	**6**	**8**
	Low (1)	**1**	**2**	**3**	**4**
		Low (1)	**Medium (2)**	**High (3)**	**Very High (4)**
		THREAT			

EXPOSURE LEVEL DESCRIPTIONS			
Level	**Score**	**Value**	**Description**
Low	**1**	1	Unlikely (<25%)
		2	
Medium	**2**	3	Limited probability of occurrence (25 - 50%)
		4	
High	**3**	5	Good probability of occurrence (51 - 75%)
		6	
		7	
		8	
		9	

Very High	**4**	10 11 12 13 14 15 16	Very high probability of occurrence (>75%)

3.0 RISK ASSESSMENT MATRIX

This matrix denotes the effect of combining the impact of a security breach (derived from the asset valuation analysis) and the likelihood of such an incident occurring (derived from the threat/vulnerability analysis). A total of 4 risk levels are defined as depicted below.

The risk levels can be further described as follows:

RISK LEVEL DESCRIPTIONS				
Level	**Score**	**Value**	**Description**	**Tolerable Frequency**
Low	**1**	1 2	These describe risks that are generally tolerable, and whose effects the Organisation can bear without significant difficulty as part of its normal operations or within a single accounting period (e.g., in any given financial year). They have minor negative impacts on the Organisation's business operations and do not require further action.	Fairly frequent
Medium	**2**	3 4	These describe risks whose effects would have a considerable impact on the Organisation in a single accounting period (e.g., any given financial year), but could be managed and become acceptable if the number of events does not become excessive and the cost could be spread over that single period. These may have significant negative effects on the Organisation's business operations. Whether or not	Occasional

			the risks should be mitigated should be considered on a case-by-case basis.	
High	**3**	5 6 7 8 9	These describe risks that are serious, whose effects would be too great for the Organisation to bear in a single accounting period (e.g., any given financial year), but would become acceptable if the cost could be spread over a sufficient period (i.e., several accounting periods). These will have serious negative effects on the Organisation's business operations and should be reduced or otherwise treated to make them more acceptable.	Infrequent
Very High	**4**	10 11 12 13 14 15 16	These describe risks that are considered intolerable and require urgent attention. They will have major negative effects on the Organisation's business and should be mitigated under all circumstances. It is crucial that all these risks are reduced or otherwise addressed to ensure they do not occur.	Rare

4.0 RISK RESPONSE OPTIONS

1. Treat

Treating the risk means that the Organisation will take measures to reduce or eliminate the risk's impact and/or likelihood. This is handled through the application of controls.

2. Tolerate/Accept

This involves the informed decision to accept a particular risk. This may occur with or without treating the risk. For instance, some risks represent such a low impact and/or likelihood that treating the risk does not represent a good return on the necessary investment.

3. Transfer

Some risks can be transferred to other parties, such as through insurance, outsourcing, and so on.

4. Terminate/Avoid

Terminating a risk means that the risk is too great to permit, but treating it is too expensive or difficult. In these instances, the Organisation chooses to find a way to completely avoid the risk itself, such as through the elimination of the asset, restructuring information infrastructure, and so on.

5.0 CRITERIA FOR PERFORMING THIRD PARTY RISK ASSESSMENTS

The Organisation shall adopt a systematic approach to third party security risk assessment in line with globally accepted standards for Information Security Management.

The following criteria shall be adopted for performing Third Party Risk Assessments:

- An initial comprehensive risk assessment covering all information assets shall be conducted.
- Planned periodic updates to the risk assessment shall be performed. These should identify changes to assets, threats, vulnerabilities, and therefore risk levels.
- Risk assessments shall be conducted as part of projects that involve significant changes to the Organisation's people, technology, processes, or general information assets.
- Risk assessments shall be performed upon major external changes affecting the Organisation, which may invalidate the conclusions from previous risk assessments, e.g., changes to applicable legislation.

5.1 RISK ASSESSMENT PROCESS AND CONSIDERATIONS

5.2 THIRD PARTY SOURCING, SELECTION & DUE DILIGENCE PROCESS

The need for the third-party engagement must be clearly defined. A business requirement or justification document that clearly defines the scope of engagement should be developed and presented to the relevant authority within the Organisation, who will review and either approve or reject the request.

- Standard criteria and methods must be considered for evaluating and selecting third parties based on their technical and functional fit for our Organisation.
- A Non-Disclosure Agreement (NDA) must be signed if there would be disclosure of the company's sensitive information, whereby the NDA serves as a legal contract that outlines

the terms and conditions under which confidential information can be shared, used, and protected.

- Requests for Proposals (RFPs) and surveys shall be communicated to potential third parties where necessary, and their responses will be assessed and reviewed to ascertain their capability, maturity level, and compliance with industry standards.

5.3 GENERAL CRITERIA TO BE CONSIDERED.

- General Security measures
- Compliance & Data Security
- Reputation & Integrity
- Track record & References.
- Expertise & Industry knowledge
- Technical Capabilities
- Financial Stability
- Location
- Cost Model & Transparency
- Compliance with Regulation

Data Center Providers & Cloud Providers	**Contractor Developers**	**Security Consultants**	**Software Development Companies for Outsourcing**	**Partners Providing Services**
Scalability Physical Security Redundancy Location Cost Model General security measures Compliance & Data Security Disaster	References Reputation & Integrity Track record Technical know-how & Industry knowledge.	References Reputation Track record Industry knowledge	References Reputation & Integrity Track record Technical know-how & Industry knowledge	References Reputation & Integrity Track record Technical know-how & Industry knowledge

Recovery and Business Continuity				

There shall be proper documentation and reporting of the findings and outcome of the third-party sourcing, selection, and due diligence processes. This will serve as documented evidence that a proper and fair process was followed, which considered risk impact analysis.

At least three (3) shortlisted proposals will be submitted for review before final approval by Top Management. Representatives from at least the following teams will be involved in the final review and approval process:

- IT Security & Compliance
- IT Infrastructure & Development
- IT Audit
- Research & Development
- Relevant Business Units.

5.4 THIRD PARTY ONBOARDING

Vendor accounts and information will be created in a vendor database upon the successful submission of all required documentation and award of initial job and thereafter assigned a vendor number which will be referenced every time a purchase order is created for such vendor, this is to provide easy tracking of vendors.

Since the requirements have been clearly defined, necessary contractual agreements and documentation should be completed by both parties. Examples of such agreements are:

- Documentation and Onboarding
- Service Level Agreements (SLAs)
- Granting access to company resources: Access to company resources will be granted as documented in the contractual documents based on scope of work.
- Security Awareness: Awareness sessions shall be conducted for all Third parties at least twice a year, for them to know, be reminded of and adhere to Organisation's security policies. Compulsory awareness must be done when a vendor is onboarded.

5.5 DOCUMENTATION AND ONBOARDING

- Background of key Shareholders, Directors, Members and Trustees.
- Qualification and experience of the Management and key Staff.
- Value and duration of contracts completed in the past as a main contractor or subcontractor.
- Persons that may be contacted for references.

5.6 MINIMUM REQUIREMENT FOR SLAS

The SLA which serves as the binding contractual agreement should consist of a minimum of the following:

- Terms of services
- Scope of services provided.
- Duration/Expiration of contract
- Termination and cancellation clause
- Performance monitoring metrics
- Penalty grids
- Escalation metrics
- Dispute resolution clause
- Confidentiality and non-disclosure clause
- Data protection clause
- Intellectual property rights
- Governing law
- Force majeure
- Right to audit

5.7 THIRD PARTY MONITORING

- Audits of third-party security controls and compliance with contractual agreements shall be conducted at least twice a year. Logical and Physical access shall also be reviewed during such audits, and reports of findings shall be presented to relevant stakeholders.
- An Incident Response Plan shall be established with Third Parties to ensure alignment with Organisation's incident management procedures.
- Performance Monitoring and Evaluation of Third-Party services shall be conducted against the terms in the SLA at least once a year, to address deviations promptly.

5.8 THIRD PARTY CLOUD PROVIDER SERVICES

Information in the cloud must be protected by appropriate security measures, as required by the associated risk. The use of cloud computing services must be supported by a contract which covers all clauses that apply to standard third-party contracts. In addition, the following special provisions related to the use of cloud services must be included:

- Providing a secure authentication service.
- Restricting access to authorised users.
- Implementing appropriate malware monitoring and protection solutions.

- Communication of security-related information about unusual or malicious activity.
- Providing advance notification prior to any changes being made to the way the service is delivered.
- Information handling requirements as described in Organisation Information Classification policy also apply to information used in the cloud.
- The use of cloud-based storage shall be restricted to the one approved by the Organisation.
- The use of cloud-based file hosting facilities will be monitored and will include spot checks by IT security & Compliance to ensure compliance.

5.9 CHANGE OF ALLOCATED RESOURCES

In cases where dedicated individuals are assigned to our Organisation during the life cycle of a project, we require formal communication in advance to prepare the necessary work resources for that replacement as we do not encourage account/password sharing. Emergency situations may be exempted.

5.10 CONTRACT TERMINATION/ EXIT STRATEGY

- Organisation's information assets, equipment and access cards provided to third party during their contract period must be returned.
- Removal of their access to all Organisation systems.
- Channel of escalation shall be documented, this in case of issues / problems after the disengagement with the third party.
- Intellectual Property (IP) rights must be clearly defined.
- Clause for renegotiation of agreements if the security / business/ legal / regulatory requirements of Organisation changes.
- Security requirements to be followed by the third party and any subcontractors post termination of the contract.
- Clause including post termination of indemnification of Organisation in case of intellectual property, legal or regulatory issues arising from a delivered product or service.