



RISK MANAGEMENT POLICY

15 Feb, 2024

1 of 12

Date of Version

Page

Document No.

RISK MANAGEMENT POLICY

Created By:	Reviewed By:	Approved By:



RISK MANAGEMENT POLICY

15 Feb, 2024

2 of 12

Date of Version

Page

Document No.

1 Introduction

Risk Management policy shall provide a top management commitment to identify, address and mitigate the risk related to information security. All risks related to Information Communication Technology will be addressed using this Risk Management Policy. This policy provides a commitment to ensure that the Information assets of Health Dynamics Pty Ltd T/A Vibe Natural Health shall be secured from external as well as internal threats by performing the activities defined in Risk Management policy.

2 Purpose

The purpose of this policy is to ensure a commitment for the guidance in establishing, implementation and maintenance of a system for Risk Management processes and assets determined as Critical and Important.

3 Scope

This policy is implemented in all sections and interest parties of Health Dynamics Pty Ltd T/A Vibe Natural Health covering under the scope of Information Security Management System.

4 Compliances

It is mandatory to comply with this policy. All information security related risks will be identified and mitigated using this policy and related risk management policy so the compliance of this policy is mandatory at all levels of Health Dynamics Pty Ltd T/A Vibe Natural Health.

5 Roles & Responsibilities

General Manager

- Ensures availability of resources to ensure successful execution of risk treatment plans
- Ensures availability of resources required to ensure planned prevention of known risks
- Ensures involvement of key personnel in performance of this policy



RISK MANAGEMENT POLICY

15 Feb, 2024

3 of 12

Date of Version

Page

Document No.

Directors and Management Staff

- Ensure their involvement, and the involvement of relevant key personnel from their respective departments, for Risk Management activities
- Ensure support of Risk Owners in treatment of risks
- Ensure immediate reporting to Risk Owners in case a control for Risk treatment fails

Process Owners

- Ensure support for Risk Owners for implementation of Risk Treatment Plans
- Ensure reporting of issues related to Risk treatment controls adopted


Risk Owners

- Ensure implementation of Risk Treatment Plan within the assigned target date
- Ensure prevention of any process interruption during implementation of Risk Treatment Plan

6 Policy Statement

Health Dynamics Pty Ltd T/A Vibe Natural Health has determined its measures against risks to physical & information security and risks related to quality, service delivery and assets functionality, through careful assessment and planning. Following measures are taken to ensure better and reliable results through these activities:

- Business Continuity Plans has developed against all the critical processes running in the organization
- Risks related to physical, information security, quality, service delivery and assets functionality has identified and corrective actions will be taken against it
- Asset Valuation performance has been evaluated and prioritized for assets involved in Critical and Important processes
- Risk Assessment is being performed for assets valued at Critical and Important
- Risk Treatment is being decided on the basis of Risk Rating, while making sure that Residual Risk is reduced to Minor based on the treatment measures adopted
- The output of Business Impact Analysis, Asset Valuation, Risk Assessment and Risk Treatment activities shall be reviewed annually or as per requirement
- Designated Risk Owners ensures that Risk treatments shall be implemented on fixed target days

	RISK MANAGEMENT POLICY		
	15 Feb, 2024	4 of 12	
	Date of Version	Page	Document No.

Management of Health Dynamics Pty Ltd T/A Vibe Natural Health has been authorized to carry out disciplinary actions against violators of this policy.

7 Action Plan for Policy Statement

- **Identification of Business Process**

Business Impact Analysis is performed against all the processes running in the organization. For this purpose, Risk Management sheet is developed. Identify all departments and processes related to them. Select the type of process in risk management sheet:

- Internal Service: An internal process, a process not directly connected to customers
- Customer Service: A process directly resulting in output for clients, or fulfilling an objective (KPI) defined by clients
- External Service: A process monitored and controlled by Health Dynamics Pty Ltd T/A Vibe Natural Health team, but executed and run by a third party

Identify the Process Owner (designation responsible for execution of process), under the Process Owner column and identify the designation responsible to look after the process in case of absence or unavailability of Process Owner, under the Deputy column.

- **Business Impact Analysis Initiation**

Initiate business impact analysis by following contractual obligations, client requirements and needs. Determine the maximum allowable downtime to recover the process or services. Choose the most appropriate downtime limit based on business or client requirements of the process.

- Less than 10 minutes
- Less than 1 Hour
- Less than 1 Day
- More than 1 Day

Choose the most appropriate choice against a process, based on the following (under Dependencies on this Process):

- One or more Projects



RISK MANAGEMENT POLICY

15 Feb, 2024

5 of 12

Date of Version

Page

Document No.

- One or more internal processes

The priority of a process is dependent on the combination of its “Tolerable Downtime” and “Dependencies on this Process”. Priority of the process can be anyone of the following based on the assessment made:

- Critical
- Important
- Normal

Priority assessment is performed based on the criteria given below:		
CRITICAL	Less than 5 Minutes	One or more Projects
	Less than 1 hour	One or more Projects
	Less than 1 day	One or more Projects
	Less than 5 Minutes	One or more internal processes
IMPORTANT	Less than one hour	One or more internal processes
	Less than 8 hours	One or more internal processes
	Less than 1 day	One or more internal processes
	More than 1 day	One or more Projects
NORMAL	More than 1 day	One or more internal processes

Asset valuation is prioritized for assets based on the Priority determined of their associated processes.



RISK MANAGEMENT POLICY

15 Feb, 2024

6 of 12

Date of Version

Page

Document No.

- **Performing Asset Valuation**

Performance of Asset Valuation is prioritized for assets involved in Critical and Important processes Access Asset Valuation Sheet. Choose the Process (priority is given to processes deemed Critical, Important, and at last Normal, respectively). Select the Information Assets involved in process delivery and mention Asset ID under the required column.

Give asset name (make, model, etc.) under the Assets column.

Select the most appropriate scores for Confidentiality (C), Integrity (I), and Availability (A);

Confidentiality	(C)	1	Unauthorized access to asset, information, process or service, or its use, is ignorable, and will not result in negatively effecting a business process, or a department's operations
		2	Unauthorized access to asset, information, process or service, or its use can lead to Noticeable negative effects on business unit (a single process, or a department), but will either have no effect or ignorable effect on services associated with customer or a critical business process
		3	Unauthorized access to asset, information, process or service, or its use can lead to noticeable negative effects on business processes or units, critical for the primary objectives of the organization, can negatively affect services associated with customers, and/or negatively affect regulatory requirements
		1	Incomplete, manipulated and/or corrupt form of asset, information, process or service, will not result in negatively effecting a business process, or a department's operations

Integrity

(I)



RISK MANAGEMENT POLICY

15 Feb, 2024

7 of 12

Date of Version

Page


Document No.

		2	Incomplete, manipulated and/or corrupt form of asset, information, process or service, can lead to Noticeable negative effects on business unit (a single process, or a department), but will either have no effect or ignorable effect on services associated with customer or a critical business process
		3	Incomplete, manipulated and/or corrupt form of asset, information, process or service, can lead to noticeable negative effects on business processes or units, critical for the primary objectives of the organization, can negatively effect services associated with customers, and/or negatively effect regulatory requirements
Availability	(A)	1	Unavailability and/or inaccessibility of asset, information, process or service, will not result in negatively effecting a business process, or a department's operations
		2	Unavailability and/or inaccessibility of asset, information, process or service, can lead to Noticeable negative effects on business unit (a single process, or a department), but will either have no effect or ignorable effect on services associated with customer or a critical business process
		3	Unavailability and/or inaccessibility of asset, information, process or service, can lead to noticeable negative effects on business processes or units, critical for the primary objectives of the organization, can negatively effect services associated with customers, and/or negatively effect regulatory requirements

The sheet will automatically determine Asset Score, which in turn will assign Asset Value without user intervention:

- **Asset Value Normal:** Score is 5 or less
- **Asset Value Important:** Score is between 6 to 7
- **Asset Value Critical:** Score is between 8 to 9

Group ID (GRID) are selected to identify and group together assets of same type and value i.e.

	RISK MANAGEMENT POLICY		
	15 Feb, 2024	8 of 12	
	Date of Version	Page	Document No.

- Assets are of same type
- Assets are of same value

The grouping of assets in this manner will support the Risk Assessment process by reducing repetitive data.

- **Determining Risks**

Risk Assessment is performed for assets valued at Critical and Important. Open Risk Assessment sheet and select the appropriate GRID (Choose the Group ID Index sheet).

Identify the Asset Type and determine the Threat and identify it under the specified column. Threat is the act, event or thing, which may exploit the corresponding vulnerability to create risk(s) to business process and assets.

Determine the Vulnerability of the assigned asset, which might be exploited by the selected Threat. Vulnerabilities are weaknesses of an asset which might be exploited by a threat and create risks in a business environment.

Describe the risks under Risk Description which may affect the business process and the asset being assessed for risks. The Risk must be created under the combination of the Threat and Vulnerability chosen. One combination of Threat and Vulnerability might lead to more than one Risks.

Choose the appropriate Existing Control based on any one of the scenarios:

- **Appropriate Control Not Applied:** In case there are no existing controls applied to mitigate the Risk, or the existing Control is insufficient and not listed.
- **Choosing a Control from the given list:** In case organization has already adopted one of the listed controls, it is selected from the given list.

- **Performing Risk Assessment**

Risk Treatment is decided on the basis of Risk Rating, while making sure that Residual Risk is reduced to Minor based on the treatment measures adopted. Give Value of the asset under V:

- Normal: 1



RISK MANAGEMENT POLICY

15 Feb, 2024

9 of 12

Date of Version

Page

Document No.

- Important: 2
- Critical: 3

Value is determined under Asset Valuation. Give chances of **Occurrence** under O:

- 1: Low
- 2: Medium
- 3: High

Give **Severity** of Impact under S:

- 1: Lowest
- 2: Moderate
- 3: Highest

The values for assessment of risk rating are adopted based on the applicability of the definitions given below:

Chances of Occurrence	(O)	1	Risk has a very least likelihood of occurrence due to already existing controls, existing technology solutions, existing applications and/or due to environmental conditions of the area where such risks do not occur
		2	Risk is likely to occur as environmental condition, technology adopted, application solutions being utilized, or the process implemented, is prone to such risks, or existing controls are not enough to reduce the risk's effects
		3	Risk has a very high likelihood of occurrence as the region is prone to such hazardous natural conditions or events / incidents, or information assets, technology and their dependencies are always under constant threat, or the existing control is not giving effective results
Severity of Consequences	(S)	1	Risk's severity is not significant enough to effect business or IMS, and can be considered tolerable, based on the existing controls



RISK MANAGEMENT POLICY

15 Feb, 2024

10 of 12

Date of Version

Page

Document No.

2

Risk's severity is significant enough to effect IMS policies and processes, and may compromise internal business processes as the existing controls are weak, but will not effect processes or information related to customers and/or regulatory bodies

3

Risk's severity is highly significant and will effect IMS policies and processes and will also effect processes connected with customers and/or stakeholders including regulatory bodies, due to missing or insufficient controls

The sheet will assess Risk Rating and give Risk Status. Risk Rating is determining the criticality of Risk:

- **Grave** Risk: Risk Score is between 15 to 18
- **Noticeable** Risk: Risk Score is between 8 to 12
- **Minor** Risk: Risk Score is 6 or Less

Whereas,


- **Grave** Risk expresses the most critical form of risk, and requires immediate attention of decision makers for timely mitigation.
- **Noticeable** Risk expresses an important form of risk, and requires a planned approach for mitigation. It is prioritized after Grave Risk.
- **Minor** Risk expresses the lowest form of risk, and requires no further action, as the organization has the capacity to bear its impact.

No further actions are required if the Risk is at Minor.

- **Risk Treatment**

Risks are accepted for Assets valued at Normal. Risks rated at Minor are accepted. Using the same Risk Assessment sheet, choose the Controls Suggested:

- Choose a Control listed in the drop-down-menu
- Choose a Custom Control if the listed controls do not include the required risk treatment measure
- Selected No Control Required, if the Risk Rating is at Minor already (no Risk Treatment is required)

	RISK MANAGEMENT POLICY		
	15 Feb, 2024	11 of 12	
	Date of Version	Page	Document No.

Note: Appropriate Control is not Applied, is not applicable at this stage. Briefly describe the implementation plan under Risk Treatment Description.

Based on the control adopted and Risk Treatment described, choose the appropriate Control Strength:

- **Manual Control:** The treatment measure adopted is controlled entirely by a human resource and his or actions. No automated solution such as software or technology has been adopted.
- **Semi-Automated:** The treatment requires the role of both human resource(s) and a semi-automated solution which can be a technology or a software solution.
- **Fully Automated:** The treatment is almost fully automated based on a technology or a software, and requires minimal human resource involvement.

Based on the Control Strength selected, Revised Risk Status will be automatically determined by the sheet.

Note: This Risk Status is not yet achieved, as it is only projecting the effects of Planned Risk Treatment measures on existing Risk Status, after the treatment has been fully implemented.

Revised Risk Status other than Minor will require reevaluation of Treatment measures adopted. Identify the Risk Owner, under the assigned column. Assign a realistic Target Date. Priority is given to Grave Risks.

Residual Risk is only accepted in Minor states. In case a Risk is at Noticeable, but the organization does not want to further invest on it, its acceptance will be signed by GM of Health Dynamics Pty Ltd T/A Vibe Natural Health.

Grave Risks are forbidden to be accepted without at least being reduced to Noticeable or Minor Risks through risk treatment controls.

- **Follow-up**

Based on the Target Date assigned, follow-up with Risk Owners and concerned BOPs, to determine the **Status** of Risk Treatment under the appropriate column:

- **Completed:** Treatment is completed on time
- **Pending:** Status is unknown, Target Date is close
- **Delayed:** Status is overdue from Target Date
- **Reassigned:** Treatment was unsuccessful



RISK MANAGEMENT POLICY		
15 Feb, 2024	12 of 12	
Date of Version	Page	Document No.

The output of Business Impact Analysis, Asset Valuation, Risk Assessment and Risk Treatment activities is reviewed annually. Designated Risk Owners ensure that Risk treatments are implemented on fixed target days

Directors and Management Staff and Group Leads ensure involvement in Risk Assessment and treatment activities to prevent occurrence of known risks