©(ORGANISATION NAME)

DISASTER RECOVERY AND BACKUP POLICY

Subject: Disaster Recovery/Business Continuity Plan and Backup Policy		Author: MuVio Solutions Ltd
Document Type: Policy (Internal)	Page: 1 of 14	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 INTRODUCTION

The prolonged unavailability of normal business services has dire consequences on the financial and reputational standing of the Organisation. It is therefore necessary to minimise interruptions to business activities.

The Organisation developed its Disaster Recovery & Backup policy to establish the requirements for maintaining effective and continuous business operations in the event of failures and disasters.

Reference	Description of Risk
SAFETag	Backup of Sensitive Data on BYOD and Office Devices
SAFETag	Operational Security and Office Mapping

1.2 APPLICATION

This policy is applicable to all employees (permanent and temporary), service providers and all critical systems and/or resources utilised by the Organisation for the execution of its business processes.

1.3 SCOPE

All human resources, critical system resources, services, and physical assets in use within the Organisation.

1.4 BUSINESS CONTINUITY PLANNING

A business continuity plan explains the actions that should be taken before, during and after unexpected events and situations. It is designed to help identify, prevent, or reduce risks where possible; prepare for risks that may be out of control; respond and recover if an incident, crisis pr disaster occurs.

1.4.1 OBJECTIVE

The objective of business continuity planning is to ensure that Business Continuity Management plans and procedures are in place to facilitate the normal functioning of the day-to-day activities in the event of failures or disasters.

1.4.2 POLICY STATEMENTS

1.4.2.1 A strategy for Business Continuity Management shall exist. This shall be approved by the management and reviewed on a predefined frequency.

1.4.2.2 The strategy for Business Continuity Management shall serve as a single framework on which business continuity plans and procedures shall be developed and adopted within the business.

1.4.2.3 Head of Departments/relevant stakeholder within the Organisation shall identify the business activities for which there is a necessity and priority for recovery, based on criticality. They also decide on the level and scope of Business Continuity Planning after fully considering business risks, impacts and legal responsibilities as well as the costs of various continuity planning options, which the Organisation may pursue.

1.4.2.4 When determining the criticality of business activities and the supporting applications, systems, and infrastructure; consideration needs to be given to the impact which the loss or unavailability of these will have, particularly in terms of the following:

- Loss of business activities and services provided to clients.
- Financial impact as determined by loss of revenue.
- Legal impacts in terms of contractual, governmental, and regulatory requirements.
- Impact on the corporate image and reputation of the Organisation.
- Interaction with other processes, services, and applications.
- Interaction with third parties.

1.4.2.5 The overall approach to be followed when developing the corresponding Business Continuity Management plans and procedures can then be established; and all system recovery and response timeframes shall be quantified.

1.4.2.6 Prior to developing Business Continuity Management plans and procedures, formal risk and impact analysis shall be performed to identify business critical processes and systems; risk analysis should consider the likelihood of a disaster or failure occurring, and its potential impact. The events should then be prioritised and addressed accordingly.

1.4.2.7 Business Continuity Management plans and procedures shall be developed to align with the agreed upon strategies; these plans and procedures shall be formally documented, communicated, and simulated throughout the Organisation and shall cover all information resources. The plans and procedures should initiate the recovery of information resources in the event of a disaster or system failure.

1.4.2.8 Business Continuity Management plans and procedures shall contain procedures to keep critical business activities and services running and shall not merely contain fallback arrangements for information resources and services. The plans and procedures shall consider, amongst others, the following:

- Identification and prioritisation of critical business processes.
- Potential impact of various types of disasters.
- Identification and agreement on the key resources and defined responsibilities.
- Emergency arrangements for accommodation and communication.

- Conditions, responsibilities, and authority for invoking emergency procedures.
- Responsibilities for staff awareness in the emergency procedures.
- Training of responsible persons.
- Testing strategies and schedules.
- Maintenance schedules.
- Relationships with other business continuity plans and procedures.
- Fall-back arrangements for computer services.
- Backup strategies and locations.
- Suppliers and support contacts (applicable to Outsourcing and Third-Party services)
- Inventory lists for hardware, software, documents and data.
- Steps for recovery of processes and systems.
- Restore to permanent facilities.
- Legal requirements.
- Security arrangements.
- Review of the plans.
- Change management procedures.
- Analysis of consequences/causes of disaster.

1.4.2.9 The Business Continuity Management Plan shall incorporate a Disaster Recovery Plan for the recovery of IT services.

- All information used in the decision-making process for continuity planning shall be formally documented (e.g. risk analysis results, insurance costs, etc.).
- Business Continuity Management plans and procedures shall include the responsibilities for carrying out effective recovery, the emergency procedures to be followed and the conditions under which these procedures shall be activated.
- Business Continuity Management plans and procedures shall contain sufficient details to permit timely resumption of business activities; the documented information shall be sufficient for the execution of the plans and procedures by the individuals responsible for recovery.
- Annual reviews shall be conducted to ensure the effectiveness of the business continuity and recovery plans of the Organisation.
- Relevant users shall be aware of their responsibilities regarding Business Continuity.
- Users shall be educated on business continuity procedures and the emergency plan.

1.4.3 INITIATING BUSINESS CONTINUITY PLAN

The following processes shall be triggered in the event of a disaster and individuals responsible for implementing recovery shall be clearly informed of their responsibilities.

- Business Continuity Management plans and procedures shall be readily available but restricted to Authorised/relevant stakeholders.
- Business Continuity Management plans and procedures shall be tested. The frequency shall be in accordance with pre-defined schedules; the simulation of continuity management plans and procedures shall be carried out, verifying that the plans and procedures are relevant and can still facilitate recovery within required timelines.
- Individual components of the business continuity management plan shall be tested frequently. Testing of the plans and procedures shall occur when there are major changes to Business operations that govern these activities. All tests, and the results thereafter, must be recorded.
- A Business Continuity Management team shall be established to coordinate business continuity issues in the event of an emergency.

2.0 DATA BACKUP/RESTORE & ARCHIVE MANAGEMENT

2.1 OBJECTIVE

The objective of this subsection is to ensure the Organisation effectively manages its data redundancy process and to protect it against loss of data.

2.2 POLICY STATEMENTS

The Organisation shall make available to the following information to ensure effective backup of their data.

- Identification of critical data, information and software that need to be backed up.
- The retention periods for backup of critical business information and archived copies.
- The frequency and type of information backup, based on the business process requirements.

2.2.1 The Organisation shall develop a Backup Strategy to effectively provide redundancies for critical business data.

2.2.2 Actions to be taken in case of temporary or permanent loss, destruction or unavailability of information shall be clearly documented, forming part of the Organisation's standards and procedures.

2.2.3 Critical data, information and software shall be backed-up, according to the backup strategy.

2.2.4 Backup and backup procedures shall be tested regularly. The frequency shall be in accordance with predefined schedules; testing procedures shall be in place to verify that backup meet business continuity requirements and that they are accessible and reliable when needed. Appropriate storage media shall be made available for both data backup and restoration.

2.2.6 Backup information and facilities shall be readily available to implement disaster recovery and restricted to Authorised employees.

2.2.7 All application data, which is required for recovery, shall be kept in a secure off-site facility; a copy of the most current critical software, application programs, documentation, and other contingency/disaster records shall also be kept off-site.

2.2.9 Copies of documentation pertaining to backup shall be stored alongside the backup.

2.2.10 A backup register shall be in place, maintained and reviewed on a regular basis; the backup register shall identify all information and systems to be backed up. It shall also include the nature, timing, and extent of backups. The register should be reviewed for completeness on a regular basis and updated whenever new systems are introduced.

2.2.11 All backup and test results of such backup shall be logged. The logs shall be reviewed on a regular basis.

2.2.12 End users shall be responsible for ensuring that data under their direct control are backed-up; this shall apply to data stored on user's PCs. Users shall ensure that the data they are responsible for are backed-up adequately and stored securely.

2.2.13 Authorised/Designated staff within the Organisation, shall be responsible for the retrieval of backup media from alternate locations.

2.2.14 The Authorised staff shall obtain approval from the designated management staff (i.e. CIO/CISO/Head of IT, or as specified) prior to the retrieval of backup media from alternate locations.

2.2.15 The Authorised staff shall return retrieved media to the alternate location not later than after 48 hours of fulfilling the purpose for which it was retrieved.

2.2.16 The Authorised staff shall sign the logbook/attendance register at the alternate location during retrieval and at the return of backup media.

2.3 BACKUP STRATEGY

The backup strategy, along with a disaster recovery plan, constitute the all-encompassing business continuity plans which is the blueprint for the Organisation to withstand a cyberattack and recover with zero-to-minimal damage to the business, reputation, and data. The backup strategy adopted is also dependent on the nature (classification) of data and applications to be backed up.

2.3.1A - DATA CLASSIFICATION

SN	Classification	Description
1	Public Data	This type of data is freely accessible to all employees and the public. It can be freely used, reused, and redistributed without repercussions. Examples are marketing materials, flyers, posters, press releases etc.
2	Internal Data	This type of data is strictly accessible to internal company personnel or internal employees who are granted access. This might include internal memos or other communications, business plans, etc.
3	Confidential Data	Access to confidential data requires specific authorisation and/or clearance. Types of confidential data might include Personally Identifiable Information, Social Security numbers, cardholder data, M&A (Mergers & Acquisitions) documents, and more. Usually, confidential data is protected by laws like HIPAA and the PCI DSS.
4	Restricted Data	Restricted data includes data that, if compromised or accessed without authorisation, could lead to criminal charges and massive legal fines or cause irreparable damage to the company. Examples of restricted data might include proprietary information or research and data protected by state and federal regulations.

2.3.1B - APPLICATION CLASSIFICATION

SN	Classification	Description
1	Mission Critical	These are important applications where failure will cause a severe impact to Organisation operations.
2	Business Critical	These are necessary applications where failure will cause significant impact to business operations. These applications usually give competitive advantage and adds to the value of the Organisation.
3	Business Important	These are applications that are enhancing in nature – “Could have”. These applications drive operational efficiency; enhance the way we work and provides automation of processes.
4	Productivity Applications	These are applications that are enticing in nature – “Nice to have”. These applications are nice to have and make work easy.

2.3.2 DAILY TASKS

The following tasks are to be performed daily:

SN	TASK	OWNER
1.	Real time data replication/backup of xxx	xx
2.	Daily backup to tape/cloud for xxx	xx

3.	Daily backup of xxx	xx
4.	Incremental backup of database xxx	xx

2.3.3 MONTHLY TASKS

The following tasks are to be performed monthly:

SN	TASK	OWNER
1.	Monthly backup of xxx	xx
2.	Monthly backup of xxx	xx

2.3.4 QUARTERLY TASKS

The following tasks are to be performed on a quarterly basis:

SN	TASK	OWNER
1.	Quarterly backup of xxx	xx
2.	Quarterly backup of xxx	xx

2.3.5 ANNUAL TASKS

The following tasks are to be performed on an annual basis:

SN	TASK	OWNER
1.	Annual/End of Year backup of xxx	xx
2.	Annual/End of Year Report generation for xxx	xx

2.3.6 RESPONSIBILITY FOR BACKUPS

a. The data owners will identify the data to be backed up.
b. The responsible stakeholder i.e. Application Manager, will schedule the backup and monitor all backup jobs.
c. The responsible stakeholder i.e. IT Team will use a combination of full and incremental backup methods.

2.3.7 TESTING THE INTEGRITY OF BACKUPS (RESTORE)

The business continuity and disaster recovery tests are to be carried out at planned intervals e.g. quarterly. During the system failover test, production servers are "demoted" while backup servers are "promoted" to production. Failover test activities are carried out by all departments to ensure the integrity of the data/databases. During this period, network traffic is directed to the disaster recovery site, whose database is activated from passive to read/write mode making it available for start-up and for users.

2.3.8 DATA RESTORATION TIME/POINT OBJECTIVES

The Recovery Time Objective/Recovery Point Objective (RTO/RPO) is a very significant part of the corporation's data protection strategy. In the event of any hardware failure and data corruption, the recovery time is defined as the time it takes to retrieve the data from any offsite location to the point of complete data restore. The point of recovery would involve that data available up to the last backup date and time.

The Recovery Time Objective/Recovery Point Objective should be within 24 hours, or as defined by the organisation. When defining the RTO and RPO, the Application classification and Data classification shall be put into consideration and used as a baseline.

2.4 RECOMMENDATIONS/ADVISORY ON BACKUPS

Organisations with 1 – 5 Staff	Organisations with 6 – 20 Staff	Organisations with more than 20 Staff
• Consider the use of free/basic cloud storage plan for backup – see examples https://www.google.com/drive/ https://onedrive.live.com/ https://www.dropbox.com/ • Consider the use of shared folder on cloud storage for backup. https://support.microsoft.com/en-us/office/share-onedrive-files-and-folders-9fcc2f7d-	• Consider the use of free/basic cloud storage plan for backup – see examples https://www.google.com/drive/ https://onedrive.live.com/ https://www.dropbox.com/ • Consider the use of shared folder on cloud storage for backup. https://support.microsoft.com/en-us/office/share-onedrive-files-and-folders-	• Consider the use of free/basic cloud storage plan for backup – see examples https://www.google.com/drive/ https://onedrive.live.com/ https://www.dropbox.com/ • Consider the use of a shared folder on cloud storage for backup.

Organisations with 1 – 5 Staff	Organisations with 6 – 20 Staff	Organisations with more than 20 Staff
de0c-4cec-93b0-a82024800c07 https://help.dropbox.com/share • Consider the use of Microsoft Windows backup. https://support.microsoft.com/en-us/windows/back-up-your-windows-pc-87a81f8a-78fa-456e-b521-ac0560e32338 • Consider the use of backup for mobile devices. https://support.apple.com/mac-backup Backup android devices	9fcc2f7d-de0c-4cec-93b0-a82024800c07 https://help.dropbox.com/share • Consider the use of drive mapped as a shared folder. • Consider the use of open-source file backup solutions. https://freefilesync.org/ https://www.borgbackup.org/ https://www.urbackup.org/ • Consider the use of Microsoft Windows backup. https://support.microsoft.com/en-us/windows/back-up-your-windows-pc-87a81f8a-78fa-456e-b521-ac0560e32338 • Consider the use of backup for mobile devices. https://support.apple.com/mac-backup Backup android devices	https://support.microsoft.com/en-us/office/share-onedrive-files-and-folders-9fcc2f7d-de0c-4cec-93b0-a82024800c07 https://help.dropbox.com/share • Consider the use of drive mapped as a shared folder. • Consider the use of business/enterprise cloud storage plan for backup. • Consider the use open-source file backup solutions. https://freefilesync.org/ https://www.borgbackup.org/ https://www.urbackup.org/ • Consider the use of a centralised file storage Server. • Consider the use of Microsoft Windows backup. https://support.microsoft.com/en-us/windows/back-up-your-windows-pc-87a81f8a-78fa-456e-b521-ac0560e32338

Organisations with 1 – 5 Staff	Organisations with 6 – 20 Staff	Organisations with more than 20 Staff
		● Consider the use of backup for mobile devices. https://support.apple.com/mac-backup Backup android devices