AMENDMENTS LOG

Revision History

Version	Revision Author	Reviewer / Approver	Date	Summary of Changes
1.0	Nor Asfiah Binte Jamalludin (ISMS MR)	James Chia (CEO)	1 Aug 2025	Initial Release

TABLE OF CONTENTS

PURPOSE

This document describes the procedure for backup and restoration of information, software and systems to enable recovery from loss of data or systems.

SCOPE

The backup and restoration plan here includes, but not limited to, operating systems, applications, and other information assets identified as critical for the organisation's operations.

REFERENCE

ISO/IEC 27001 Standard Annex A 8.13 Information backup

RESPONSIBILITIES & AUTHORITIES

Top Management has the prime responsibility and approval authority for this control.

MR/IT shall ensure that backup copies are maintained and regularly tested.

PROCEDURE

A. Backup Plan

The organisation shall provide means to restore the integrity of information in the event of a hardware/software failure, and to provide a measure of protection against human error or the inadvertent deletion of important information, and determine and meet any requirements (e.g., contractual and/or legal requirements) regarding the frequency of backups, type of backups, the frequency of reviews and tests of backup, the recovery procedures, and any requirement for the archival, retention, and erasure/disposal contained in information held for backup requirements.

All employees are advised to ensure that they store their critical files on the designated cloud folders assigned to them for backup. For software products, the organisation will rely on the cloud backup services.

B. Loss of Data

- If loss of data is discovered, evaluation and investigation by MR/IT is immediately dispatched.
- In most cases, loss of data is related to file corruption, virus, security or human error.
- Once the problem has been determined, the organisation will proceed with the restoration of data from backup copies.

- Any loss of data related to file corruption, virus, security or human error will be logged and addressed as an incident in line with *ISMS-ORG-10 Information Security Event and Incident Management.*

C. Restoration of Data

- The organisation will determine the time and date of the lost data.
- The organisation will determine the appropriate backup to restore the lost data.
- The most current backup will be located for restoration.
- The organisation will monitor the restoration process.
- Upon restoration, the organisation will evaluate the integrity of the restored data.
- For occasions where personal data needs to be restored, perhaps due to a system malfunction, attack or disaster, personal data restoration process shall ensure that the personal data is restored into a state where its integrity can be assured, and/or where inaccuracy and/or incompleteness is identified and can be resolved. The procedure for, and a log of, personal data restoration efforts shall be maintained. At a minimum, the log of the restoration efforts should contain the name of the person responsible for the restoration and a description of the restored personal data.

D. Testing of Backup

Backup measures for information, systems and services will be tested at least once a year to ensure that they meet the objectives of incident response and business continuity plans. The test will be combined with the business continuity and disaster recovery plan testing in line with *ISMS-ORG-11 Business Continuity & Disaster Recovery.*