4. Policy: Backup and Restoration

4.1. PURPOSE

The Company set is responsible for ensuring the confidentiality, integrity, and availability of the data and information stored on its systems. The backup and restoration of data is an important aspect to ensure the availability of information and data for the Company.

4.2. OBJECTIVE

The objective of this Policy is to formalise the backup and restoration process adopted by the Company. The process of backing up data is pivotal to a successful Disaster Recovery Plan (DRP).

4.3. SCOPE

This Policy applies to employees, contractors, visitors, and other persons (User) authorised to access and use the Company's systems. This Policy covers all servers, workstations, network devices, operating systems, applications, and other information assets belonging to the Company.

4.4. TERMS AND ABBREVIATIONS

- **Backup** means the copying of physical or virtual files or databases to a secondary location for preservation to assist in the event of equipment failure or catastrophe.
- **Restoration** means the process of restoring something to its former condition and, in the case of a computer or other electronic device, means returning it to a previous state, including restoring a previous system backup or the original factory setting, or restoring data that was on the system.

4.5. POLICY

The extent, frequency and retention period of backups must reflect:

- The Company's business requirements.
- The Company's security requirements of the information involved.
- How critical the information is to the Company's continued business operations.
- The retention period for essential business information.
- Any requirement for archived copies to be permanently retained by the Company.

The extent, frequency and retention periods of the Backups must be reviewed regularly. The Company's critical systems must be clearly identified, and the Backup arrangements must cover all system information, applications, and data necessary to recover the complete system in the event of a disaster. Where backup arrangements are automated, such automated solutions must be sufficiently tested prior to implementation and at regular intervals thereafter.

All backup media must be labelled with dates and codes which enables easy identification of the source of the data and the type of backup used on the media.

Where the confidentiality of the information is important, backups must be protected by encryption and all encryption keys must be always kept securely. Clear procedures must be in place to ensure that backup media can be decrypted as required.

Complete records of the backup copies must be retained both locally and remotely and afforded physical and environmental protection. Such records should include information pertaining to the data location, date of backup, type of backup and the like. Copies of backup media must be removed from all Company devices as soon as reasonably possible when a backup or restoration has been completed.

Backup media, which is retained on-site at the Company, must be stored securely at a sufficient distance away from the original data source to ensure that both the original and backup copies are not compromised. Access to the backup media must be restricted to authorised staff only. All backups identified for long term storage must be stored at a secure remote location with appropriate protection to ensure continuing media integrity.

Restoration processes must be checked and tested regularly to ensure that they are effective and that they can be completed within the time allotted in the operational procedures for recovery.

Hard copy paper files containing important information and data must also be digitised (scanned) and stored in a location where they will be backed up by the Company in the same manner as electronic information.

Backup data and media no longer required, must be clearly marked and recorded for secure disposal or destruction, with due environmental consideration.

4.6. PROCEDURE

There are 5 common types of backups:

Full Backup	A Full Backup is when every single file and folder in the Company's systems is backed up. A Full Backup takes longer and requires more space than other types of backups. However, the process of restoring lost data from the backup is much faster
Incremental Backup	With Incremental Backups only the first backup is a Full Backup. Subsequent backups only store changes that were made after the previous backup. The process of restoring lost data from the backup is longer, however, the backup process itself is much quicker.
Differential Backup	A Differential Backup is like an Incremental Backup. With both, the first backup is full and subsequent backups only store changes made to files after the last backup. This type of backup requires more storage space than an Incremental Backup does, however, it also allows for a faster restoration time.
Mirror Backup	A Mirror Backup is when an exact copy is made of the source data. The advantage of Mirror Backups is that old, obsolete files are not being stored. When obsolete files are deleted, they are also deleted from the Mirror Backup when the system backs up. The disadvantage of a Mirror Backup is that, if files are accidentally deleted, they may also be lost from the backup.
Replication Backup	A Replication Backup occurs where data stored on servers is replicated between different servers. Sometimes these servers may be in the same data centre. If the backup is a pure replication, there is a risk that if the data on the main server is corrupted, the rest of the replicated data could also be corrupted. When implementing Replication Backups, a backup that is at least 1 day older than the live data must be kept managing this risk.

4.7. BACKUP SCHEDULE

The Backup schedule of the Company must be reviewed and updated on a regular basis. The Backup Schedule must contain the following information:

- The system and device to be backed up.
- The location of such device.
- The type of backup that was implemented.
- The frequency of the backup
- The person responsible for the backup.

4.8. USER'S RESPONSIBILITIES

- Users must ensure that data is securely maintained and is available for backup.
- Users must store any data and files that require backup on their allocated network storage area and not on local hard drives.
- If the allocated storage area becomes unavailable, Users may not temporarily save the data locally on hard drives or on a USB data stick.

4.9. DATA RESTORATION

Data Restoration must only be done by competent, authorised staff within the Company.

4.10. EMPLOYEE ACKNOWLEDGEMENT

As a requirement of IT system access, and as a component of security awareness training, all Users, whether employees of the Company or third parties, will be required to provide signed acceptance of this Policy, confirming such User's acknowledgement that they are bound by all provisions set out in this Policy. A copy of the signed document will be provided to the User in question, and the original will be retained by the Company.

4.11. RIGHTS RESERVED BY THE COMPANY

The Company reserves the right to monitor, audit, screen, and preserve Company information as the Company deems necessary, to maintain compliance with these Policies and all relevant provisions of the Promotion of Access to Information Act 4 of 2013 (POPIA). Any distribution, unauthorised use, or benefit from Company information by an employee or user, in contravention of these Policies may result in disciplinary action being taken by the Company. The use of any system in such a way that breaches any of the provisions of these Policies, will be reported to the Information Officer at the Company, which may lead to further disciplinary action being taken.

4.12. ENFORCEMENT AND POTENTIAL DISCIPLINARY ACTIONS

Any violation of these Policies may result in disciplinary action being taken against the employee or user in question. Such disciplinary action will be taken in accordance with the Company's disciplinary code and may include the termination of employment for employees of the Company, or cancellation of contractual relations in the case of other users, such as contractors or consultants.

4.13. POLICY AWARENESS AND UPDATE

Training and awareness:

The requirement for these Policies will be explained in detail in the Company's induction program, in the case of employees of the Company. Further training regarding these Policies will be offered from time to time by the Company. The Company will specifically make users who are not employees of the Company aware of these Policies.

Dissemination:

These Policies will be made available on the Company's website, intranet, or notice boards.

Review:

These Policies will be reviewed from time to time to ensure ongoing compliance with POPIA. Such revisions will take place at least annually.

4.14. INTERNAL DOCUMENT APPROVAL

Information Officer Name	Signature	Date
Paula Gageiro		23 June 2021

4.15. DOCUMENT VERSION CONTROL

Version	Date	Summary of Changes