



Backup and Restoration Policy and Procedure

1. SCHEDULE	2
2. BACKUP SCHEDULE.....	2
3. RETENTION PERIOD SCHEDULE	2
4. INTRODUCTION	2
5. OBJECTIVE.....	3
6. SCOPE	3
7. TERMS AND ABBREVIATIONS	3
8. DOCUMENTS	3
9. POLICY.....	3
10. PROCEDURE.....	4
11. RIGHTS RESERVED BY THE ORGANISATION.....	5
12. ENFORCEMENT AND POTENTIAL DISCIPLINARY ACTIONS	5
13. POLICY AWARENESS AND UPDATE.....	6

Initial
SS
Initial

1. SCHEDULE

1.1	The Organisation	Insight Business Accounting
1.2	Registration number	20/02/2022
1.3	VAT registration number	4670306416
1.4	Physical address	191 Vinko Street, Pretoria, Gauteng
1.5	Email address	Shane@insightba.co.za

2. BACKUP SCHEDULE

System/device	Location	Type of Backup	Frequency	Person responsible for Backup

3. RETENTION PERIOD SCHEDULE

System/device	Location	Type of Backup	Retention period

4. INTRODUCTION

- 4.1. The Organisation set out in item 1.1 of the Schedule (“**Organisation**”) is responsible for ensuring the confidentiality, integrity, and availability of the data and information stored on its systems.
- 4.2. The Backup and Restoration of data is an important aspect to ensure the availability of information / data for the Organisation.

SS

Initial

5. OBJECTIVE

The objective of this policy and procedure ("**Policy**") is to formalise the Backup and Restoration process adopted by the Organisation. The process of Backing up data is pivotal to a successful disaster recovery plan ("**DRP**").

6. SCOPE

- 6.1. This Policy applies to (i) employees, (ii) contractors, (iii) visitors, and / or (iv) other persons authorised to access and use the Organisation's systems ("**Users**").
- 6.2. This Policy covers all servers, workstations, network devices, operating systems, applications and other information assets belonging to the Organisation.

7. TERMS AND ABBREVIATIONS

- 7.1. In this Policy, in addition to the other terms that have been defined in the body of the Policy, the Organisation makes use of the following terms:
 - 7.1.1. "**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;
 - 7.1.2. "**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 (i) restoring a previous system backup or the original factory setting, or (ii) restoring data that was on the system;
 - 7.1.3. "**CIO**" means the chief information officer of the Organisation; and
 - 7.1.4. "**IT User**" means a User within the Organisation authorised to be responsible for the carrying out of the Organisation's necessary information technology ("**IT**") functions.
- 7.2. In addition, unless the contrary is specified, terms that are used in the Policy that are specifically defined in POPIA, are given the meanings ascribed to them in POPIA.

8. DOCUMENTS

This Policy should be read in conjunction with the Organisation's Acceptable Usage Policy insofar as it relates to IT aspects.

9. POLICY

- 9.1. The extent, frequency and retention period of Backups must reflect:
 - 9.1.1. the Organisation's business requirements;
 - 9.1.2. the Organisation's security requirements of the information involved;
 - 9.1.3. how critical the information is to the Organisation's continued business operations;
 - 9.1.4. the retention period for essential business information; and
 - 9.1.5. any requirement for archived copies to be permanently retained by the Organisation.
- 9.2. The extent, frequency and retention periods of the Backups must be reviewed regularly and in each case where circumstances change or failures occur.
- 9.3. Backup arrangements must meet the requirements of the Organisation's business continuity plans.
- 9.4. The Organisation's critical systems must be clearly identified and, for such systems, the Backup arrangements must cover all system information, applications, and data necessary to recover the complete system in the event of a disaster.
- 9.5. Where Backup arrangements are automated, such automated solutions must be sufficiently tested prior to implementation and at regular intervals thereafter.
- 9.6. All Backup media must be appropriately labelled with dates and codes / markings which enables easy identification of the original source of the data and the type of Backup used on the media.
- 9.7. Where the confidentiality of the information is important, Backups must be protected by encryption and all encryption keys must be kept securely at all times, with clear procedures in place to ensure that Backup media can be promptly decrypted as required.
- 9.8. Accurate and complete records of the Backup copies must be retained both locally and remotely and afforded the same level of physical and environmental protection as other important documentation. Such records should include information pertaining to the department in question, data location, date of Backup, type of Backup and the like.

Initial
SS
Initial

- 9.9. Copies of Backup media must be removed from all Organisation devices as soon as reasonably possible when a Backup or Restoration has been completed.
- 9.10. Backup media which is retained on-site at the Organisation, prior to being sent for storage at a remote location, 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.
- 9.11. Access to the retained Backup media must be restricted to authorised staff only.
- 9.12. All Backups identified for long term storage must be stored at a secure remote location with appropriate environmental control and protection to ensure continuing media integrity.
- 9.13. Backup media must be protected in accordance with the Organisation's physical, environmental, data protection and media handling policies and procedures.
- 9.14. 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.
- 9.15. Hard copy paper files containing important information and data must also be digitised and stored in a location where they will be Backed up by the Organisation in the same manner as electronic information.
- 9.16. Where Backups fail, data and system owners must be promptly informed and a record maintained. Such a record must include information regarding any action taken by the Organisation to address such failure.
- 9.17. Backup data / media no longer required must be clearly marked and recorded for secure disposal or destruction, with due environmental consideration.
- 9.18. Where provision is made in this Policy for reviews to be done at regular intervals, such intervals will be determined by the CIO in his / her sole discretion.

10. PROCEDURE

- 10.1. There are 5 (Five) common types of backup, they are:
 - 10.1.1. **Full Backup:** A full Backup is when every single file and folder in the Organisation'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.
 - 10.1.2. **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.
 - 10.1.3. **Differential Backup:** A differential Backup is similar to 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.
 - 10.1.4. **Mirror Backup:** A mirror Backup is when an exact copy is made of the source data. The advantage of mirror Backups as opposed to full, incremental, or differential 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 if the deletion is not discovered prior to the next scheduled Backup.
 - 10.1.5. **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 (One) day older than the live data must be kept to manage this risk.
- 10.2. **Backup schedule:** Item 2 of the Schedule sets out the Backup schedule of the Organisation, which must be reviewed and updated on a regular basis. Item 2 includes the following information:
 - 10.2.1. The system / device to be Backed up;
 - 10.2.2. The location of such device;
 - 10.2.3. The type of Backup that was implemented, including:
 - 10.2.3.1. full Backup;
 - 10.2.3.2. incremental Backup;
 - 10.2.3.3. differential Backup;
 - 10.2.3.4. mirror Backup; and / or
 - 10.2.3.5. replication Backup;
 - 10.2.4. The frequency of the Backup; and

Initial
SS
Initial

10.2.5. The person responsible for the Backup.

10.3. **Retention period of Backups:** Item 3 of the Schedule sets out the retention periods of Backups implemented within the Organisation. This schedule must be reviewed and updated on a regular basis. Item 3 includes the following information:

10.3.1. The system/device Backed up;

10.3.2. The location of such device;

10.3.3. The type of Backup that was implemented, including:

10.3.3.1. full Backup;

10.3.3.2. incremental Backup;

10.3.3.3. differential Backup;

10.3.3.4. mirror Backup; and / or

10.3.3.5. replication Backup; and

10.3.4. The retention period of the Backup in question.

10.4. **IT Users responsibilities**

10.4.1. IT Users must ensure that data is securely maintained and is available for Backup at all times.

10.4.2. IT Users must store any data / files that require Backup on their allocated network storage area and not on local hard drives.

10.4.3. If the allocated storage area becomes unavailable, IT Users may not temporarily save the data locally on hard drives or on a USB data stick, but must promptly contact the CIO to Restore the data in question.

10.5. **Data Restoration**

10.5.1. Data (file) Restoration must only be done by competent, authorised staff within the Organisation.

10.5.2. The following procedure must be followed when performing Restorations:

10.5.2.1. IT Users must request the Restoration of data by contacting the CIO;

10.5.2.2. The CIO must verify that the IT User has permission or authorisation to view or Restore data prior to any Restoration taking place;

10.5.2.3. The CIO must request the following information from the IT User in order to facilitate the Restoration:

10.5.2.3.1. The reason for the Restoration;

10.5.2.3.2. The names of files or folders to be Restored;

10.5.2.3.3. The original location of the files or folders to be Restored;

10.5.2.3.4. The IT User's best estimation of the date and time when the IT User noticed the deletion / corruption in question; and

10.5.2.3.5. The IT User's best estimation of the date and time when the IT User recalls the files or folders in question being accessible and intact;

10.5.2.4. Requests from third party software / hardware vendors for file or system Restorations for the purpose of system support, maintenance, testing or other unforeseen circumstance must be made to the CIO;

10.5.2.5. IT Users accessing Backup media for the purpose of a Restoration must ensure that any media used is returned to a secure location when it is no longer required; and

10.5.2.6. A log must be maintained to record the use of Backup media whenever it has been requested and / or removed from secure storage.

11. RIGHTS RESERVED BY THE ORGANISATION

The Organisation reserves the right to monitor, audit, screen, and preserve Organisation information as the Organisation deems necessary, in its sole discretion, in order to maintain compliance with this Policy and, by extension, all relevant provisions of the Promotion of Access to Information Act 4 of 2013 ("POPIA"). Any dissemination, unauthorised use or benefit from any Organisation information by a User in contravention of this Policy may result in disciplinary action being taken against such User by the Organisation. Furthermore, the use of any account or system in such a way that breaches any of the provisions of this Policy will be reported to the appropriate supervisor or manager within the Organisation, which may lead to further disciplinary action being taken.

12. ENFORCEMENT AND POTENTIAL DISCIPLINARY ACTIONS

Any violation of this Policy may result in disciplinary action being taken against the User in question. Such disciplinary action will be taken in accordance with the Organisation's applicable disciplinary code, and may include the (i) termination of employment in relation to employees of the Organisation, or (ii) cancellation or termination of contractual relations in the case of other Users, such as contractors or consultants.

Initial
SS
Initial

Notwithstanding the foregoing, should any authorised User fail to adhere to this policy, the individual will be dealt with as prescribed by the Organisation's disciplinary code and procedures.

13. POLICY AWARENESS AND UPDATE

- 13.1. **Training and awareness:** The (i) requirement for, and (ii) a User's obligation in terms of, this Policy will be explained in detail in the Organisation's induction program, in the case of employees of the Organisation. Further training and additional awareness regarding the Policy will be offered from time to time by the Organisation. The Organisation will specifically make Users who are not employees of the Organisation aware of the Policy.
- 13.2. **Dissemination:** This Policy will be made available on the Organisation's network, intranet or similar portals.
- 13.3. **Review:** This Policy will be reviewed from time to time in order to ensure ongoing compliance with POPIA, but such revisions will take place at least annually. More frequent review may be required in response to (i) exceptional circumstances, (ii) organisational change, or (iii) relevant changes in legislation or guidance.

Initial
SS Initial