

Data Backup Policy

BITS Technology Group Pty Ltd

Action	Name	Title
Prepared By	Muhammad Nauman Mustafa	Cyber Security Engineer
Reviewed By	Blair Munro	Head of Technology
Approved By	Bernard Mangelsdorf	Chief Executive Officer

Version	Date	Description of Change	Updated By
1.0	12 March 2025	Initial Policy Creation	Muhammad
1.2	28 May 2025	Applications were added	Muhammad
2.0	24 June 2025	Updated the retention and frequency of backups	Muhammad

1. Purpose

This document outlines the data backup process and status for key BITS Technology Group applications and infrastructure. The purpose of this document is to communicate to the BITS team the importance of current and timely backups and to set expectations.

2. Process Flow

The following high-level steps are followed by the BITS team:

1. **Identify Critical Data and Systems:** Determine which data and systems are essential and need to be backed up.
2. **Schedule Regular Backups:** Set up a schedule for regular backups (e.g., daily, weekly) based on the criticality of the data.
3. **Perform Backups:** Execute the backup process according to the schedule. The application custodian would be responsible for the manual backups.
4. **Store Backups Securely:** Ensure backups are stored in a secure, offsite location and only the application custodian (refer to RBAC Matrix) or user nominated by the custodian has access to the backup.
5. **Test Backup and Recovery Procedures:** Regularly test the backup and recovery procedures (yearly or on discretion of the leadership team/custodian) to ensure data can be restored successfully.
6. **Document and Review:** Keep detailed documentation of backup procedures and schedules and review them annually.

3. Backups

All required components of critical infrastructure in use at BITS Technology Group are backed up. Given the diverse nature of the platforms in use at BITS Technology Group, there are multiple methods of backing up data. The table 1 outlines the platform, the method, and the retention period for backups.

No	Software	Backup Platform	Frequency	Retention
1	Microsoft Resources	Cove	Weekly	365 Days
2	Microsoft Configurations	Inforcer	Daily	365 Days
3	Xero	Ledgerscope/OneDrive (manual)	Daily	180 Days

No	Software	Backup Platform	Frequency	Retention
4	IT Glue	OneDrive (manual)	Weekly	365 Days
5	NinjaOne	OneDrive (manual)	Weekly	365 Days
6	Accele	OneDrive (manual)	Weekly	365 Days

Table 1

Other applications/systems listed in Asset Register are deemed to non-critical for the business (do not host business critical data) thus, does not need to be backed up.

4. Retention

Data being backed up by operational systems are not intended to be a repository for individual system settings or configuration changes; they are backups of whole systems or applications that can be used in the event of failure to restore back to a point in time.

5. Removal

The retention period in this document is intended to be a minimum value for the length of time backups are retained for documented systems. Some systems might have backups stored for longer than the retention period in this document; however, when removing old backups, only the value above will be retained.

6. Review and Compliance

- **Review:** This policy will be reviewed annually and updated as necessary to ensure its continued relevance and effectiveness.
- **Compliance:** Compliance with this policy will be monitored through regular audits and reviews. Non-compliance may result in disciplinary action.