

Backup Plan Policy

Prepared by: Max.chan@mediaworld.com.hk

Approved by:

Date: 2026-01-15

Organization: Tree (tree.com.hk)

Effective Date: 2026-01-15

Version: BP-v1.0

1. Purpose

This policy defines how Tree (tree.com.hk) protects business data through regular backups and recovery procedures.

2. Scope

This policy applies to data on all Tree (tree.com.hk) systems:

System	Data Covered
File Server	Shared documents, departmental files, and user personal folders
QuickBooks	Accounting records, invoices, financial reports
POS System	Sales transactions, receipts, inventory data (Visa card payments via payment gateway — not stored locally)
Online Sales System	Online orders, customer orders, product listings (Visa card payments via payment gateway — not stored locally)

Note: Office PCs (tree.com.hk) are **not** backed up directly. User work files must be saved to the **file server personal folder** to be included in backup.

Payment gateway: All **Visa card payment information** is handled entirely by the **payment gateway** and is **not stored** in Tree's systems.

3. Policy

3.1 Backup Strategy

All critical business data must be backed up using a **two-copy** approach:

Copy	Location	Purpose
Copy 1 — Local	On-site at Tree premises (local backup storage)	Fast recovery for day-to-day restores
Copy 2 — Cloud	Off-site cloud data center	Protection against local disaster, theft, or hardware failure

- All backups are kept in **local** storage and the **cloud data center**.
- Both copies must be updated on the same daily backup schedule.
- Local and cloud backups must be kept separate from the primary production system.
- Backup copies must be protected from unauthorized access, loss, and corruption.

3.2 Systems Covered

System / Data	Local	Cloud Data Center
File Server (including user personal folders)	Daily	Daily
QuickBooks	Daily	Daily
POS System	Daily	Daily
Online Sales System	Daily	Daily

3.3 Retention

- Backups are retained for **7 days** in both **local** storage and the **cloud data center**.
- Backups older than 7 days must be securely deleted automatically or by IT.

3.4 Recovery and DR Testing

Routine recovery

- Local backup should be used first for routine recovery; cloud backup is used when local copy is unavailable.
- Recovery steps must be documented and available to authorized IT staff.
- In the event of data loss, recovery must be started as soon as possible.

Yearly DR test

- A **Disaster Recovery (DR) test** must be performed **at least once per year**.
- The DR test is **file-based** — IT restores sample files from backup (local and/or cloud) and verifies the files are complete and usable.
- DR test results must be documented (date, files tested, source — local or cloud, pass/fail).
- Any issues found during the DR test must be investigated and resolved by IT.

3.5 Responsibilities

- **IT Team:** Configure, monitor, and maintain local and cloud backup systems; perform the **yearly file-based DR recovery test**.
- **System Owners:** Identify critical data and confirm both backup copies are running.
- **End Users (tree.com.hk):** Save all important work to their **file server personal folder**. Files stored only on the local office PC are **not backed up** and may be lost.

4. Exceptions

Any exception to this policy must be approved by management and documented with a reason and expiry date.

5. Review

This policy will be reviewed at least once per year or when systems change significantly.