

Data Classification and Data Backup 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: DCB-v1.0

1. Purpose

This policy defines how Tree (tree.com.hk) protects and backs up company data. Tree does not use formal data classification levels — all business data is treated with the same level of protection and backup.

2. Scope

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

System	Data Covered
File Server	Shared documents, departmental files, and user personal folders
QuickBooks	Financial and accounting data
POS System	Sales and transaction records (Visa card payments via payment gateway — not stored locally)
Online Sales System	Online orders and customer data (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**. Tree (tree.com.hk) systems **do not store** card or payment details on the file server, QuickBooks, POS, or online sales systems.

3. Data Handling

- Tree does **not** operate a formal data classification scheme (e.g., Public / Internal / Confidential).
- All company data on the systems listed above is considered **business data** and must be handled with care.
- End users (tree.com.hk) should not share company data outside the organization without management approval.
- Sensitive information (e.g., passwords, customer personal data) must not be stored on personal devices or unapproved services.
- **Visa card payment information** is processed by the **payment gateway** only and must **not** be stored in Tree's systems.

4. Data Backup Requirements

All business data is backed up daily. Each backup is kept in **two locations**:

Copy	Storage Location
Copy 1 — Local	On-site at Tree premises (local backup storage)
Copy 2 — Cloud	Off-site cloud data center

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

4.1 Backup Security

- All backups are kept in **local** storage and the **cloud data center** only.
- All backup copies are **secured** and protected from unauthorized access, loss, and corruption.

- **Only IT administrators** may access backup data for restore, maintenance, or monitoring purposes.
- End users and other staff **do not** have access to backup systems or backup copies.
- Backups are retained for **7 days**, then securely deleted.

4.2 DR Recovery Test

- A **Disaster Recovery (DR) test** is performed **yearly** to confirm backups can be restored.
- The test is **file-based** — sample files are restored from backup and verified by IT.
- DR test results are documented and kept on record.

4.3 General Rules

- Data must be stored on the **file server** or approved systems — not only on local office PCs.
- **QuickBooks**, **POS**, and **online sales** data must be included in the company backup plan.
- Backup copies must be stored separately from the primary production system — one copy on **local** storage, one copy in the **cloud data center**.

5. Responsibilities

- **IT Team:** Manage backups, secure backup access (IT administrator only), perform restores when requested, and conduct the **yearly file-based DR recovery test**.
- **Management:** Approve any exception to this policy.
- **End Users (tree.com.hk):** Save work to the **file server personal folder** and report data loss to IT immediately.

6. Review

This policy will be reviewed at least once per year.