

System User Access Management 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: SUA-v1.0

1. Purpose

This policy ensures that access to Tree (tree.com.hk) systems is granted only to authorized users, based on job needs, and removed when no longer required.

2. Scope

This policy applies to user accounts and access for:

System	Access Type
File Server	Shared folders, departmental drives, user home folders
QuickBooks	Accounting modules based on job role
POS System	Cashier, supervisor, and admin access levels
Online Sales System	Order management, product admin, reporting
Office Users + PCs	Local user login (standard user, no admin rights); tree.com.hk email and office applications

Also covers network login, VPN, and remote access where applicable.

3. Policy

3.1 Account Provisioning

- New user accounts are created only after approval from the user's manager or HR.
- Each office user is assigned a **local user account** on their PC (standard user — **no administrator rights**).
- **QuickBooks**, **POS**, and **online sales** accounts are granted separately based on job role.
- Tree operates a **closed internal system** with a relatively **flat role structure**. Access is assigned based on job function and business need; where systems support it, permissions are kept to the minimum required for daily duties.

3.2 Authentication

- Strong passwords must be used according to company standards.
- Multi-factor authentication (MFA) should be enabled if the application supports it, especially for remote access and admin accounts.
- Passwords must not be shared with others.

3.3 Access Review

- User access should be reviewed periodically (at least once per year), taking into account the flat structure of the organization.
- Managers should confirm that team members still require their current access.
- Access that is clearly no longer needed should be removed where practical.

3.4 Access Changes

- Role changes, transfers, or promotions require an access update request.
- Temporary access (e.g., for contractors) must have a defined end date.

3.5 Access Termination

- When a user leaves Tree (tree.com.hk) or changes roles, access must be disabled on:
 - Office PC / tree.com.hk account
 - File server folders
 - QuickBooks, POS, and online sales system (as applicable)
- HR or the user's manager must notify IT promptly for offboarding.
- All company devices and credentials must be returned or revoked.

3.6 Privileged Access

- **Office users do not have administrator rights** on their PCs and cannot install software or change system settings.
- Software installation and system changes on office PCs are performed by **IT only**.
- Administrator and elevated-access accounts must be limited to authorized IT staff.
- Admin accounts should not be used for daily routine work.
- Privileged access must be logged and reviewed regularly.

4. End User Responsibilities (tree.com.hk)

- Protect login credentials and report suspected compromise immediately.
- Lock workstations when away from the desk.
- Do not attempt to install software or change PC settings — request IT for any software needs.
- Use access responsibly within the closed internal environment.
- Report if you can see data or systems you should not have access to.

5. Responsibilities

Role	Responsibility
HR / Manager	Request account creation, changes, and termination
IT Team	Provision, review, and revoke access; enforce authentication standards
End Users (tree.com.hk)	Safeguard credentials and use access appropriately

6. Review

This policy will be reviewed at least once per year.