Internal IT Audit Report

Daakye Oil Palm Plantations Ltd.

Prepared by: Elijah Quarshie

Date: 7/05/2025

# 1. Audit Objectives & Goals

- Assess the effectiveness and security of the IT infrastructure across the main office and 8 remote locations.  
- Evaluate the reliability of network connectivity, server management, and endpoint devices.  
- Ensure compliance with internal IT policies, data protection regulations, and cybersecurity best practices.  
- Identify risks and vulnerabilities related to internet access, CCTV systems, access points, and data backups.  
- Review the adequacy of disaster recovery and business continuity plans.

# 2. Scope of Audit

- Main Office (13 users)  
- One physical server  
- 8 remote sites (connected to the main office)  
- Network infrastructure (routers, access points)  
- CCTV across stores and entrances  
- Training center (12 rooms, projector)  
- Security post and physical access controls  
- Printers, workstations, and backup procedures

# 3. Risk Assessment Report

|  |  |  |  |
| --- | --- | --- | --- |
| Asset/Area | Risk | Impact / Likelihood | Mitigation/Control |
| Network Server | Hardware failure, no redundancy | High / Medium | Backup server or cloud replication; UPS installation |
| Remote Sites Connectivity | Downtime due to ISP failure or VPN issues | Medium / High | Failover ISPs or LTE backups |
| CCTV System | Unauthorized access or data tampering | High / Medium | Secure with firewall, strong passwords, audit |
| Access Points (Wi-Fi) | Unauthorized Wi-Fi access | High / High | WPA3 encryption, MAC filtering, VLAN segmentation |
| User Devices (PCs) | Malware or lack of updates | High / Medium | Endpoint security, patch management |
| Printers | Data leak from unmonitored printing | Medium / Medium | Print auditing, secure release printing |
| Training Center Projector | Improper use or lack of maintenance | Low / Medium | Scheduled maintenance, restricted access |
| Data Backup | No offsite/automated backup | High / Medium | Automate local & cloud backups; test recovery |
| Security Post | Poor access control or surveillance gaps | Medium / Medium | CCTV review policy, badge logs, alerts |

# 4. Control Categories

a. Access Controls  
- Role-based access to systems and resources.  
- VPN required for remote access.  
- Biometric or ID-based physical entry at the main office.  
  
b. Network Controls  
- Routers secured with complex passwords and firmware updates.  
- Separate VLANs for users, IoT (CCTV), and guests.  
- Encrypted VPNs connecting remote locations.  
  
c. Data Backup & Recovery  
- Server backups scheduled daily (locally) and weekly (cloud).  
- Data recovery drills conducted semi-annually.  
  
d. Software Management  
- Centralized update policy using Group Policy or RMM tools.  
- Licenses tracked and renewed timely.  
  
e. Security Monitoring  
- CCTV recordings stored and backed up.  
- Audit logs enabled for server and firewall.  
  
f. Training and Awareness  
- Quarterly training for users on phishing, secure browsing.  
- Posters and reminders across office spaces.

# 5. Compliance Checklist

|  |  |  |
| --- | --- | --- |
| Control | Compliant (Y/N) | Comments/Findings |
| Server has backup and UPS |  | UPS exists but backup process unverified |
| Secure remote access via VPN |  | In use; audit access logs |
| CCTV system uses strong credentials |  | Default credentials changed |
| Wi-Fi has WPA2/WPA3 with password policies |  | WPA2 active, consider upgrading to WPA3 |
| Antivirus/endpoint protection installed |  | Needs centralized logs |
| Data backups automated and stored offsite |  | Weekly cloud backup incomplete |
| Software and OS regularly updated |  | Needs patch policy documentation |
| Printer usage logged or secured |  | Not monitored; recommend print server |
| Staff trained on cybersecurity annually |  | Initial training done, no refresher yet |
| Physical security controls at main office |  | Security post manned; no entry logbook |

# 6. Recommendations

1. Implement centralized logging for user activity and network events.  
2. Establish a business continuity plan including disaster recovery for the server.  
3. Formalize an IT policy manual and conduct periodic awareness training.  
4. Upgrade wireless security and segment IoT/CCTV traffic on a separate network.  
5. Conduct internal audits bi-annually and remediate issues timely.