Ref . No.	FP-020

FARM PRICE HOLDINGS BERHAD
[Registration No. 202301019404 (1513326-T)]
(Incorporated in Malaysia)

DATA BACKUP AND DATA RESTORATION POLICY

1.0 OVERVIEW

This Data Backup and Data Restoration Policy ("**Policy**") defines the backup policy for data within Farm Price Holdings Berhad ("**the Company**").

2.0 PURPOSE

This Policy is designed to protect the Company's data so that it is not lost and can be recovered in the event of an equipment failure, international destruction of data, or during disaster.

3.0 SCOPE

This Policy applies to data owned and operated within the Company.

4.0 DEFINITIONS

- **Backup**
  The saving of files onto online and offline mass storage media for the purpose of preventing loss of data in the event of equipment failure or destruction.

- **Restore**
  The process of bringing online or offline storage data back and putting it on an online storage system such as a File Server.

- **Archive**
  The saving of old or unused files onto offline mass storage media for the purpose of permanent storage.

5.0 TYPES OF BACKUPS AND DATA

The Company will perform the following types of backups:-

- Local Server;
  - Autocount (accounting software)
  - SQL Payroll (HR and payroll software)

- External Hard Disk.
  - Autocount (accounting software)

6.0 TIMING

- Local Server
  - Schedule backup is performed automatically at 10pm until finished, on daily basis.
  - Full schedule backup is performed automatically at 10pm until finished, monthly.

- External Hard Disk
  - Manual backup is performed by Account personnel for Autocount, weekly.

7.0 RESPONSIBILITY

The appointed IT personnel and Account and Finance Manager are responsible to ensure daily backups are performed.

8.0 ONSITE BACKUP STORAGE

- Local Server is located at onsite office (The Company's Headquarter).
- External Hard Disk shall be kept in Account Department Office.

9.0 BACKUP STORAGE ACCESS

Backup storage media can only be accessed by the discretion of Senior Finance Manager and appointed IT personnel.

10.0 RESTORATION

Users must submit an official request to the IT personnel for restoration (with Manager's approval).

11.0 GOVERNANCE AND CUSTODIAN OF THIS POLICY

11.1 The Head of IT or any designated officer identified by the Managing Director shall be the custodian of this Policy and be responsible to propose any update to this Policy for the consideration of the Audit and Risk Management Committee ("**ARMC**"), in tandem with the advent of technology and/or technological trend.

11.2 In line with the recommendation by the Malaysian Code on Corporate Governance, cyber security shall be one of the key risk areas and formed part of the Company's internal control and risk management framework. As the designated Board Committee overseeing the risk management framework of the Group, the ARMC shall oversee the governance and relevance of this Policy.

12.0 PERIODIC REVIEW

This Policy shall be reviewed from time to time by the Board (vide the ARMC) when deem necessary.

13.0 EFFECTIVE DATE

This Policy is effective 30 June 2023.

History:-

Document No.	Version No.	Board's Approval Date	Effective Date
FP-020	1.0	30 June 2023	30 June 2023

- The rest of this page has been intentionally left blank -