Ref . No.	FP-019

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

IT SECURITY POLICY

1. COMPUTER ACCESS

Data is easily leaked or transferred out by users without a proper data control in the computer. Portable storage device such as Universal Serial Bus ("**USB**") thumb drive and external hard disk are commonly used to copy out sensitive information. In order to control the transfer of data to other devices, all computers have been restricted access as follows, unless been allowed by the Management:-

- No external storage access via USB connection
- No optical drive access such as Compact Disk (CD)/Digital Versatile Disk (DVD)
- No shared folder in computer

In addition, computer must be configured with auto lock screen feature if idle for a period of time. This will prevent unauthorised uses of the computer by outsider when the user is away from the computer. Active desktop and laptops must be secured if left unattended.

Whenever possible, this policy should be automatically enforced. Access to assets is forbidden for non-authorised personnel. Granting access to the assets involved in the provision of a service must be done through the approved Service Request Management and Access Management processes.

2. COMPUTER SECURITY

Computers without a proper security protection are vulnerable to risks such as virus infection, hacking and etc. At minimum, anti-virus software must be installed in all computers. All Windows Personal Computer ("**PC**") must also be kept updated with the latest Windows update to fix any vulnerability in the Operating System. This should be done automatically via the Windows Update.

Users themselves also have a role to play to protect the computer security. Every user's account must not have any administrator right to prevent them from installing unauthorised software. Users must be educated to have some awareness about their action that could expose the computer to potential security risks. Some good practices include:-

- Do not expose own computer password to another colleague
- Do not click any attachment or link from unknown email
- Do not click any link in unknown website
- Do not register company email account in non-working related website
- Scanning technologies for virus and malware must be in place in client's PCs and servers to ensure the maximum protection in the ingoing and outgoing email.
- Security incidents must be reported and handled as soon as possible according to the Incident Management and Information Security processes. Users should not try to respond by themselves to security attacks.

3. INTERNET ACCESS

In accessing Internet, users must behave in a way compatible with the prestige of Farm Price Holdings Berhad ("**the Organisation**" or "**the Company**"). Attacks like denial of service, spam, fishing, fraud, hacking, distribution of questionable material, infraction of copyrights and others are strictly forbidden.

A gateway firewall must be configured to restrict website access. Malicious website or nonproductive websites or social medias such as Instagram, Facebook or YouTube must be blocked. Access to those blocked websites can only be granted upon approval from the Management. Internet traffic should be monitored at firewalls. Any attack or abuse should be promptly reported to the IT Team.

Internet access is mainly for business purpose. Some limited personal navigation is permitted if in doing so, there is no perceptible consumption of the Organisation's system resources and that the productivity of the work is not affected. Personal navigation is discouraged during working hours.

4. SERVER SECURITY

All servers must be protected physically and remotely to prevent unauthorised access. All servers must be placed inside the server room and the server room must be locked all the time. Access into the server room can only be granted by person in charge. Server login must also be protected with a strong password and changed yearly. A password considered strong after fulfilling all the criteria below:-

- Alphanumeric character (alphabet and number)
- At least have 8 characters
- At least have 1 capital alphabet
- At least have 1 symbol character

5. NETWORK SECURITY

A network firewall (software or hardware appliance) is needed to separate internal network and external network. All network devices must be placed behind the firewall.

Firewall can only be accessed by authorised IT administrators. IT administrators must review the firewall logs on monthly basis for any authorised access or attack such as Distributed Denial-of-Service (DDoS) or Brute Force.

Firewall will also be used to control the Internet access for all computers in internal network. Access to any website after been approved by the Company will be configured and applied through the firewall rules for each hierarchy of users.

6. EMAIL

All the assigned email addresses, mailbox storage and transfer links must be used only for business purposes in the interest of the Organisation. Occasional use of personal email address on the Internet for personal purpose may be permitted if in doing so, there is no perceptible consumption in the Organisation's system resources and the productivity of the work is not affected.

- Use of the Organisation resources for non-authorised advertising, external business, spam, political campaigns, and other uses unrelated to the Organisation business is strictly forbidden.
- In no way may the email resources be used to reveal confidential or sensitive information from the Organisation outside the authorised recipients for this information.

- Using the email resources of the Organisation for disseminating messages regarded as offensive, racist, obscene or in any way contrary to the law and ethics is absolutely discouraged.
- Use of the Organisation's email resources is maintained only to the extent and for the time is needed for performing the duties. When a user ceases his/her relationship with the Company, the associated account must be deactivated according to established procedures for the life cycle of the accounts.
- Outbound messages from corporate users should have approved signatures at the foot of the message.
- Attachments must be limited in size according to the specific procedures of the Organisation. Whenever possible, restrictions should be automatic enforced.

7. CARE OF ASSETS

- Users shall maintain the assets assigned to them clean, free of dusts and free of accidents or improper use. They shall not drink or eat near the equipment.
- The IT Team are the sole responsible for maintaining and upgrading configurations. None other users are authorised to change or upgrade the configuration of the IT assets. That includes modifying hardware or installing software.
- Special care must be taken for protecting laptops, tabs and other portable assets from being stolen. Be aware of extreme temperatures, magnetic fields, hits and falls.
- When travelling by land, sea or plane, portable equipment like laptops and tabs must remain in possession of the user as hand luggage or proper bag with protection and security.
- Losses, theft, damages, tampering or other incident related to assets that compromises security must be reported as soon as possible to the IT Team and HR.
- Disposal of the assets must be done according to the specific procedures for the protection of the information. Assets storing confidential or sensitive information must be physically destroyed or erased in the presence and arrangement of IT Team member before disposing.

8. GOVERNANCE AND CUSTODIAN OF THIS POLICY

8.1 The Head of IT or any designated officer identified by the Group 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.

8.2 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.

9. PERIODIC REVIEW

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

10. EFFECTIVE DATE

This Policy is effective 30 June 2023.

History:-

Document No.	Version No.	Board's Approval Date	Effective Date
FP-019	1.0	30 June 2023	30 June 2023

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