FAMAX TECHNOLOGY (M) SDN. BHD. (200601028954 (748710-K))

INFORMATION SECURITY POLICY

Policy Statement

Famax Technology (M) Sdn. Bhd. is committed to protecting its information assets against all internal and external threats, whether deliberate or accidental.

Purpose

To establish the management direction and principles for protecting the confidentiality, integrity, and availability of information assets in accordance with ISO/IEC 27001.

Scope

This policy applies to all employees, contractors, temporary staff, and third parties who access company information or information systems.

1. Principles

a) Information shall be protected based on its classification and business value
b) Security controls shall be applied proportionately to risks
c) Legal, regulatory, and contractual obligations shall be met
d) Information security is a shared responsibility

2. Responsibilities

a) Management shall support and enforce this policy
b) Employees shall comply with all information security requirements
c) The IT / ISMS function shall implement and maintain security controls
d) Compliance Violation of this policy may result in disciplinary action and/or legal consequences.

3. Acceptable Use Policy

3.1 Purpose

To define acceptable and unacceptable use of company IT resources.

3.2 Scope

All users of company-owned or company-managed IT assets.

3.3 Acceptable Use Users shall:

a) Use IT resources primarily for authorized business purposes
b) Protect company devices from loss, theft, or damage
c) Lock devices when unattended
d) Follow all security instructions and guidelines

3.4 Unacceptable Use Users shall not:

a) Install unauthorized software
b) Access illegal, offensive, or inappropriate content
c) Bypass security controls
d) Use company systems for personal gain or unlawful activities

Monitoring The Company reserves the right to monitor IT usage where legally permitted.

4. Access Control Policy

4.1 Purpose

To ensure access to information systems is restricted to authorized users only.

4.2 Scope

All systems, applications, networks, and data.

4.3 Policy Rules

a) Access shall be granted based on the principle of least privilege
b) User access shall be approved by management
c) Shared accounts are prohibited unless explicitly approved
d) Access rights shall be reviewed periodically
e) Access shall be removed immediately upon employment termination or role change

User Responsibilities Users are responsible for all activities performed using their accounts.

5. Password & Authentication Policy

5.1 Purpose

To protect systems and data through secure authentication mechanisms.

5.2 Scope

All users accessing company systems.

5.3 Password Requirements

Passwords shall:
a) Be at least **8 characters** (or company-defined standard)
c) Include a combination of letters and numbers (or stronger if required)
d) Not be reused across systems
e) Not be shared or written down

5.4 Authentication

a) Multi-factor authentication (MFA) shall be used where applicable
b) Default passwords must be changed immediately

5.5 Compromise

Any suspected password compromise must be reported immediately.

6. Data Protection & Classification Policy

6.1 Purpose

To ensure information is classified and handled appropriately to prevent unauthorized disclosure.

6.2 Scope

All information created, processed, stored, or transmitted by the Company.

6.3 Information Classification

Information shall be classified as:
a) Public – Approved for public release
b) Internal – For internal use only
c) Confidential – Restricted access, sensitive information

6.4 Handling Requirements

a) Confidential information must not be shared without authorization
b) Sensitive data shall be protected during storage, transmission, and disposal
c) Personal data shall be handled in accordance with PDPA Malaysia

Disposal Information shall be securely disposed of when no longer required.

Lee Chie Siang
Managing Director
01st January 2026