



FAMAX

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

Data Security Policy

1. General Use and Ownership

1.1. Proprietary Information:

All proprietary information belonging to Famax Technology (M) Sdn Bhd, stored on electronic and computing devices owned or leased by Famax Technology, employees, or third parties, remains the exclusive property of Famax Technology. Employees must uphold this ownership through legal or technical means.

1.2. Reporting:

Employees are obligated to promptly report any instances of theft, loss, or unauthorized disclosure of Famax Technology's proprietary information.

1.3. Authorized Access:

Employees may access, use, or share Famax Technology's proprietary information only within the scope of authorized and necessary fulfilment of assigned job duties.

1.4. Personal Use:

Employees are expected to exercise judgment regarding the reasonableness of personal use. Individual departments should establish guidelines for personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should adhere to departmental guidance, seeking clarification from their supervisor or manager when in doubt.

1.5. Monitoring and Auditing:

For security and network maintenance purposes, authorized individuals within Famax Technology may monitor equipment, systems, and network traffic at any time. Famax Technology reserves the right to conduct periodic audits of networks and systems to ensure compliance with this policy.

2. Security and Proprietary Information

2.1. Device Compliance:

All mobile and computing devices connecting to the internal network must adhere to the Minimum Access Policy.

2.2. Password Security:

System-level and user-level passwords must meet strong password criteria. Providing access to another individual, whether intentional or through failure to secure access, is strictly prohibited.

2.3. Screen Security:

All computing devices must be secured with a password-protected screensaver with automatic activation set to 10 minutes or less. Employees must lock the screen or log off when the device is unattended.

2.4. Communication Disclaimer:

Employee postings from an Famax Technology's email address to newsgroups should include a disclaimer stating that expressed opinions are strictly personal and not necessarily reflective of Famax Technology, unless the posting is part of business duties.

2.5. Email Attachment Caution:

Employees are required to exercise utmost caution when opening email attachments from unfamiliar senders, as these attachments may potentially harbour malicious software.

3. Unacceptable Use

3.1 Unauthorized System Access:

Attempting to access IT systems, databases, or networks without proper authorization or exceeding assigned privileges.

3.2 Malicious Software Deployment:

Introducing, disseminating, or executing any form of malicious software, such as viruses, worms, or malware, within the IT infrastructure.

3.3 Illegal Content Handling:

Uploading, downloading, or distributing illegal, obscene, defamatory, or copyright-infringing content using IT resources.

3.4 Cyber Harassment:

Engaging in cyberbullying, harassment, or discriminatory behaviour through IT channels or platforms.

3.5 Unauthorized Data Sharing:

Sharing sensitive or confidential IT-related information without the appropriate permissions.

3.6 Network Disruption Tactics:

Deliberately engaging in activities that disrupt the normal functioning of the IT network, causing excessive bandwidth consumption or performance degradation.

.....
Lee Chie Siang
Managing Director
01st January 2025