Information Security and Privacy Protection Management Framework

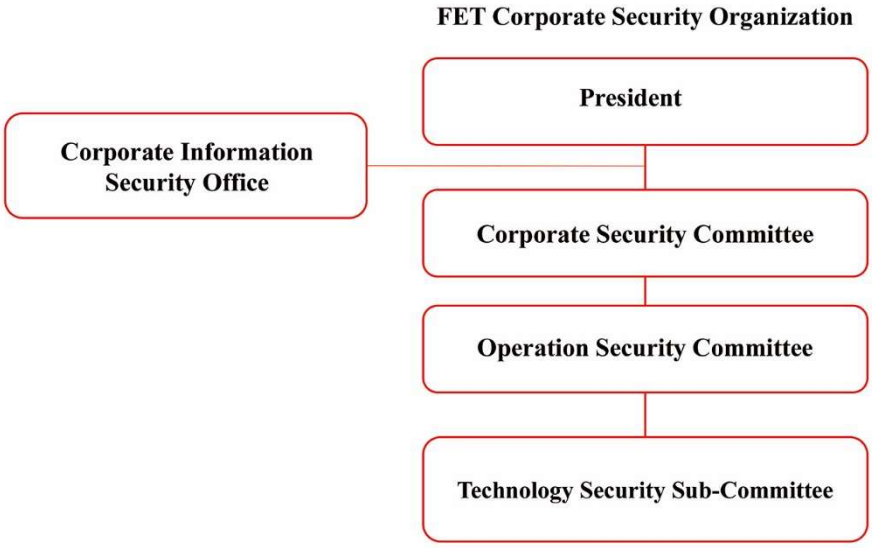
Information Security Risk Management Framework

To demonstrate its emphasis on and commitment to information security and customer privacy, FET has set forth its vision of information security: "treasuring customer trust, protecting customer information, winning the trust of customers, and maintaining sustainable services." Following these principles, FET has established corporate security organization. It has more than 30 members including the President and the representatives from all business units. Moreover, FET has set up a dedicated security department - Corporate Information Security Office and Chief Information Security Officer (CISO). The CISO, being assigned and directly report to the President, is responsible for facilitating and supervising the company's information security and personal information protection affairs as well as coordinating cross-divisional roles and responsibilities.

Information Security Policy

FET has set security policies and the objectives of “construct secured and reliable networks, ensure business continuity and resilience, comply with the laws and regulations, and guarantee the security of user’s privacy information”, with consideration given to government regulations, personal data protection, risk and crisis management. The relevant policies and regulations are regularly reviewed and revised according to internal and external requirements, including operational information security, technical security, physical security, and personnel security management. FET also conducts security risk assessments annually to identify high-risk issues such as cyberattacks, and incorporates the assessments result into annual plans by taking countermeasures of risk avoidance, risk reduction, and/or risk transfer to manage relevant risks.

The Corporate Security Organization and Responsibilities



The Corporate Security Organization consists of the representatives of business units, who are responsible to implement security management within the business unit based on their duties, so as to ensure the management and maintenance of company-wide information security.

Organization	Responsibility
Corporate Security Committee	Establish corporate security policies and governance framework, approve security plans and resource budgets, and oversee the Company's overall security risks; the Committee also has a Chief Information Security Officer (CISO) who is responsible for promoting and supervising the Company's information security and personal information security related matters.
Operation Security Committee	Establish corporate security objectives; manage the planning, establishment, implementation and review of security-related policies and regulations; and plan resources and response plans based on risk projects.
Corporate Information Security Office	Assist in the formulation of security policies; responsible for policy and awareness promotion and security committee operations.
Technology Security Sub-Committee	Review and evaluate information security risks in the technology domain and establish appropriate control measures to ensure the protection of information assets and a sound information security environment.

Solid Management Programs and Devoted Resources

In 2022, FET has held 4 meetings of Corporate Security Committee and 6 meetings of Operation Security Committee. The major discussion topics including security policy review and revision, global major risks, threats, and trend analysis, relevant regulation review such as the revision of Cyber Security Management Act (CSMA), high-risk issues identification, the response strategies and reinforcement plans. For high-risk issues, it is also regularly reported to the board members in the Risk Management Committee and then reported to the board of directors.

To continuously improve overall security, the relevant divisions had planned and completed a number of projects in 2022, including the enhancement of cyberattack protection, physical security management, the drills of business continuity plans, and the optimization of security monitoring and defense-in-depth protection mechanism. Through big data analysis, FET integrate internal and external joint defense organizations' security intelligences and strengthen high-risk alert mechanism to achieve 7x24 real-time detection, response and handling. On the other hand, FET also continually evaluates the necessity of cyber insurance to optimize the allocation of resources.

For shaping the security awareness and culture, FET has set up a dedicated area on intranet website to promote. In 2022, FET has conducted two security trainings for all employees, including "Personal Data Protection Act (PDPA) case analysis" with totally 5,369 participants and "Information Security Protection Fundamentals" with totally 5,300 participants. (The number includes both full-time and contract staffs).

Furthermore, in order to provide customers with a secured service environment and to continuously enhance and cultivate employees' security technology capabilities, FET also conducted professional and

functional trainings for dedicated cyber security and information personnel, with a view to incorporating information security control measures into all stages of the Secure Software Development Life Cycle (SSDLC) and to strengthen overall security and resilience.

To ensure the appropriateness and effectiveness of information security management and personal data protection mechanism, FET continuously pay attention to international trends and standard requirements, regularly conduct international standard verification through external third-party organizations every year, actively review and constantly enhance.

2022 Information Security and Personal Data Protection Certification	
ISO 27001 Information Security Management Certification	FET has obtained the certification for 18 consecutive years, with scope covering both mobile and fixed network services processes, including service activation, change of service, billing and payment, customer service, the development and maintenance of operations support systems, as well as the operation management of internet data centers, etc.
ISO 20000 IT Service Management Certification	FET has obtained the certification for 14 consecutive years.
BS 10012 Personal Information Management Certification	FET has obtained the certification for 10 consecutive years, with scope covering all retail stores in Taiwan, the processes of service application, customer data collection, billing and data processing, etc.
CSA STAR Cloud Security Certification	FET has obtained the highest recognition of Level-2 CSA STAR certification for 9 consecutive years.
ISO 27017 Cloud Service Information Security Certification	FET has obtained the certification for 4 consecutive years.
ISO 27018 Cloud Personal Information Protection Certification	FET has obtained the certification for 4 consecutive years.