Information Security and Privacy Risk Management Framework

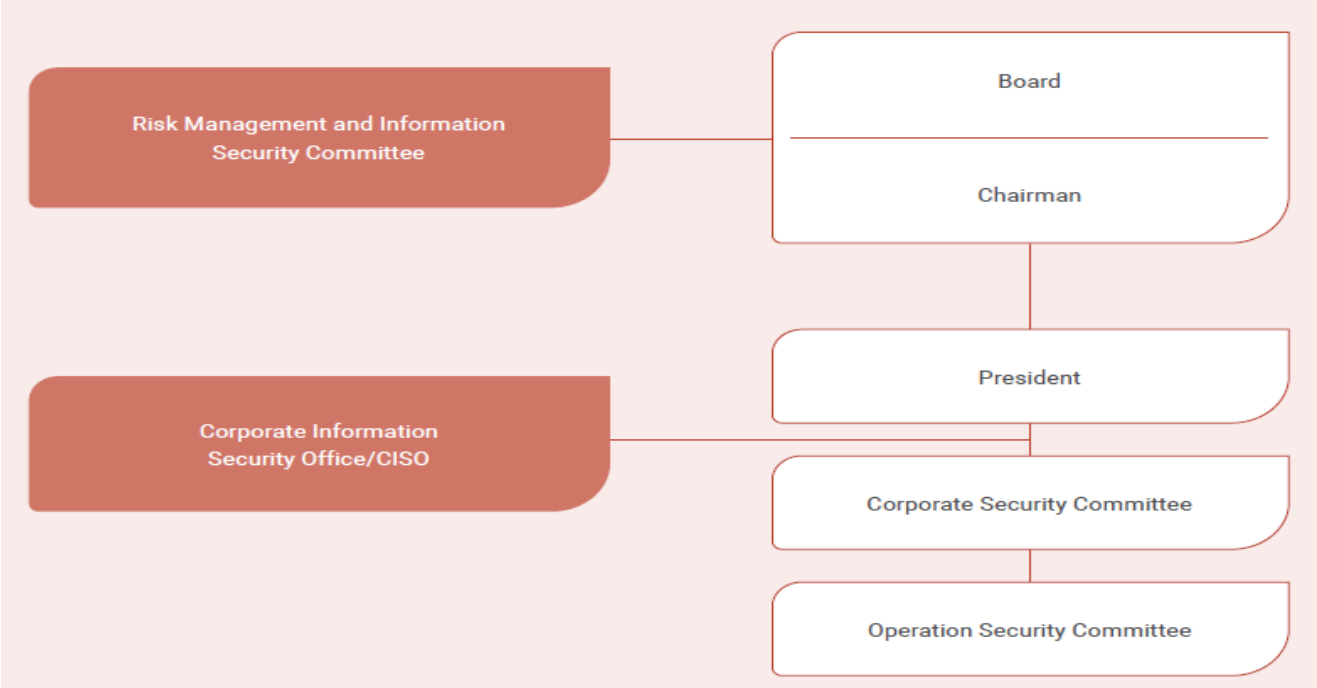
Information Security and Privacy Risk Management Organization

To demonstrate our commitment to information security and customer privacy, FET has established the information security organization. On May 3, 2024, the Board of Directors further resolved to rename the “Risk Management Committee” (RMC) to “Risk Management and Information Security Committee” (RMSC). The Committee is responsible for regularly reviewing information security and privacy protection strategies, key projects, and management effectiveness. In addition, the management organization includes more than 30 representatives from all divisions, the President, Corporate Security Committee, and Operations Security Committee. Besides, FET has set up a dedicated security department - Corporate Information Security Office and the Chief Information Security Officer (CISO). The CISO is assigned and directly reports to the President. Through the committees at all levels to promote and advocate information security and privacy protection within all divisions, and coordinate the roles and responsibilities across divisions, to ensure the effective implementation, management and maintenance of the company's overall information security.

Information and Cyber Security Policy

FET has formulate information and cybersecurity policies (see official website/Corporate Governance, link), with consideration given to government regulations, personal information 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 every year to identify major 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.

Information Security Organization and Responsibilities



Organization	Responsibilities
Risk Management and Information Security Committee	Review information security and privacy protection strategies, major plans and management effectiveness and periodically report to the Board.
Corporate Security Committee	Establish corporate security policies and governance framework, approve security plans and resource budgets, and oversee the Company's overall security risks
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 - Chief Information Security Officer (CISO)	The CISO is appointed by the President and is responsible for promoting and supervising the Company's information security and personal information security related matters. The Corporate Information Security Office assist in the formulation of security policies; responsible for policy and awareness promotion and security committee operations.

Solid Management Programs and Devoted Resources

In 2025, 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), risk issues identification, the response strategies and reinforcement plans. For major risk issues, it is also regularly reported to the board members in the Risk Management and Information Security 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 2025, 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 integrates internal and external joint defense organizations' security intelligences and strengthens 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 2025, FET has conducted two training courses for all employees, including "Personal Data Privacy Protection and De-identification Processing" and "Defense Techniques against Social Engineering Attacks", and the passing rates all achieved 100%. (All trainings include 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.

2025 Information Security and Personal Data Protection Certification	
ISO 27001 Information Security Management Certification	FET has obtained the certification for 21 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. The latest valid date of this certification is from April 29, 2025 to April 30, 2027.
ISO 20000 IT Service Management Certification	FET has obtained the certification for 17 consecutive years.

BS 10012 Personal Information Management Certification	FET has obtained the certification for 13 consecutive years, with scope covering all retail stores in Taiwan, the processes of service application, customer data collection, billing and data processing, etc.
ISO 29100 Privacy Protection Framework Certification	In 2025, FET passed the certification with scope covering mobile customers' data de-identification processing and marketing analysis operations, etc.
CSA STAR Cloud Security Certification	FET has obtained the highest recognition of Level-2 CSA STAR certification for 12 consecutive years.
ISO 27017 Cloud Service Information Security Certification	FET has obtained the certification for 7 consecutive years.
ISO 27018 Cloud Personal Information Protection Certification	FET has obtained the certification for 7 consecutive years.