Strategy 5 Integrity Governance

Key Action Aspects ① Uphold anti-corruption and integrity in business operations and implement internal control mechanisms

2025 Objectives	Status	Short-term Targets (2026)	Medium-term Targets (2027-2030)	Long-term Targets (2031-2050)
Uphold integrity governance • Notify directors and supervisors to comply with the Integrity Governance Principles for Directors and Supervisors; continue to require directors and supervisors to strictly avoid conflict of interest and unjust enrichment.	✓ Completed	• Urge compliance with the Integrity Governance Principles for Directors and Supervisors to avoid of conflict of interest in accordance with Article 206 of the Company Act.	• Continue to require directors and supervisors to strictly avoid conflict of interest and unjust enrichment in accordance with the Integrity Governance Principles for Directors and Supervisors.	• Strengthen the supervisory function of the board and improve management efficiency.

Key Action Aspects ② Strengthen information security management to ensure operation continuity

2025 Objectives	Status	Short-term Targets (2026)	Medium-term Targets (2027-2030)	Long-term Targets (2031-2050)
Strengthen information security • Comply with the Cyber Security Management Act and relevant laws, information security policies of the FSC, plus ISO 27001 and other international standards. • In accordance with the FSC's reference guide on financial zero trust architecture, assess the industry's familiarity with the model, formulate a blueprint for introducing zero trust architecture, and promote its adoption.	✓ Completed	• Continue to comply with the Cyber Security Management Act and relevant laws, information security policies of the FSC, plus ISO 27001 and other international standards. • Continue to follow the FSC's reference guide on financial zero trust architecture and gradually introduce zero trust architecture into high-risk areas of information safety control. Achieve level three of the security operation center (SOC); in 2025, the prioritization of impact sites and adoption of relevant measures have attained level one.	• Continue to comply with the Cyber Security Management Act and relevant laws, information security policies of the FSC, plus ISO 27001 and other international standards. • Continue to follow the FSC's reference guide on financial zero trust architecture and gradually introduce zero trust architecture into high-risk areas of information safety control.	• Continue to comply with the Cyber Security Management Act and relevant laws, information security policies of the FSC, plus ISO 27001 and other international standards.