Announcement

RE: Appointment of IT & Security Committee

In order to effectively manage and improve the IT & security management of Siam Makro Group as well as to support decision-making for the Siam Makro Group's committees related to IT & security topics e.g., Crisis Management Committee, Risk Management Committee, Personal Data Protection Act (PDPA) Committee, Audit Committee etc. Hereby, see as appropriate to form and appoint the following executives to IT & Security Committee:

1.	Paul Stephen Howe	Chairman
2.	Tirayu Songvetkasem	Vice Chairman (Digital systems)
3.	Suparat Sumnienghong	Committee (Operations Support & Compliance)
4.	Rattaya Ngernbumroong	Committee (Finance)
5.	Chakkit Chatupanyachotikul	Committee (Digital business)
6.	Chakarin Jiaranaipanich	Committee (QA & Privacy)
7.	Jumras Sae-yang	Committee (Infrastructure) and Secretary
8.	Head of Information Security (or representative)	Committee (Cyber Security) and Secretary

The role and responsibility of this committee is to:

1. Prepare and approve information technology and security policies and standards. Moreover, this committee has responsibility to govern and consider the exemption or waiver of compliance with information technology and security policies and standards.
    - Provide, revise, and review/test the policy regards IT & Security policy and standard
    - Make the decision to proceed or restrain any business activity that may impact to IT & Security practice of the company or related rules and regulations
    - Consider the appropriateness of compliance with information technology and information security policies and standards for projects or changes that are important to the Siam Makro Group's operation.
    - Monitor, consider exemptions or waivers, and acknowledges the results of IT & Security policy and standard in the company
    - Consider on any conflict in regards to the policy.
2. Manage information technology (IT) and security risk such as Digital transformation, Cyber Security, and System Stability and Resilience
    - Provide strategic directions in managing IT & Security risk
    - Assess and monitor the IT & Security risk, plan to mitigate the unacceptable risks, and monitor the risks based on defined KRI.
    - Report the result of IT & Security Risk Management to Siam Makro Risk Management Committee as a quarterly basis
3. Be the contact center to do IT business continuity management with tasks as below;
    - Prepare, review, and approve disaster recovery plans (DRP)
    - Assess the impact of the information technology event
    - Control and order to reduce the severity and impact of the incident situation. They will coordinate with incident response and recovery teams and other agencies from Makro and third-party vendors
    - Summarize all events that happened, and report critical or latest situations to the Crisis Management Committee for acknowledgment and making a decision to enable Business Continuity Management Plan for IT events

- Follow up on the result of using the disaster recovery plans (DRP) and report the results to the Crisis Management Committee. and the Risk Management Committee for acknowledgment

4. Be the contact center to support IT & Security audit from internal and external audit team with tasks as below;
    - Allocate resources and follow up on the IT & Security audit project's progress
    - Review and approve the IT & Security finding's details and mitigation plan (management response)
    - Direct monitor and evaluate the result of audit findings' remediation plan, and report the results to the Internal Audit Committee for acknowledgment.
5. Be the contact center to support the PDPA topics related to IT & Security with tasks as below;
    - Assess privacy controls related to IT& Security, and then plan to improve the controls to comply with Personal Data Protection Act (PDPA).
    - Allocate resources and follow up on the progression of PDPA project related to IT & Security
    - Direct monitor and evaluate the result of privacy controls and issues, and report the results to the PDPA Committee for acknowledgment.
6. Perform other duties as assigned

Effective from 2 December 2021