INFORMATION TECHNOLOGY SECURITY POLICY

Introduction

Thai Beverage Public Company Limited and its subsidiary companies ("**ThaiBev**") realizes the importance and value of its information systems and its processing resources, both manual and automated. Taking account of this importance, ThaiBev is committed to ensuring the confidentiality, integrity, and availability of its information and information systems and to take the necessary action to ensure that suitable controls are in place to provide an adequate level of protection.

Scope of the Policy

The Information Technology Security Policy ("Policy") which includes information security and cybersecurity applies to all directors, executive officers and employees of the companies in ThaiBev, and contractual/temporary workers, contractors, or anyone employed on behalf of ThaiBev.

1. Definitions

1.1 "**Chief Information Officer**" (CIO) means executive officer responsible for the management, implementation and usability of information and computer technologies.

1.2 "**Chief Information Security Officer**" (CISO) means executive office responsible for information security and cybersecurity.

1.3 "**IT**" means information technology.

1.4 "**IT Managers**" means IT managers responsible for the respective IT functions or IT within the respective entities.

1.5 "**IT Administrators**" means IT staffs and administrators who are authorized to manage the systems.

1.6 "**Users**" means all directors, executive officers, employees and contractual/temporary workers of entities within ThaiBev, and other persons or entities who use ThaiBev's computer resources and IT infrastructure.

2. Policy

2.1 ThaiBev shall establish a set of principles, rules, standards, procedures and guidelines to protect ThaiBev's IT assets and resources from unauthorized access, accidental or intentional disclosure, and destruction to minimize disruption to business activities.

2.2 ThaiBev shall set a clear direction and demonstrate support for, and commitment to, information security through the issue and maintenance of an IT Security Regulation across the organization.

2.3 ThaiBev management shall implement suitable controls to achieve information security, including specific rules, standards, procedures, organizational structures, and software functions.

3. Roles and responsibilities in IT Security

3.1 **IT Administrators** are responsible for knowing and enforcing IT security rules, standards, and procedures.

3.2 **IT Managers** are responsible for ensuring that IT Administrators are aware of their day-to-day security responsibilities as well as IT security rules, standards, and procedures that might apply for securing information systems.

3.3 **Chief Information Security Officer (CISO)** is responsible for updating IT security rules, standards, and procedures with the latest developments and best practices.

3.4 **Chief Information Officer (CIO)** is responsible for reviewing and approving IT security rules, standards, and procedures to ensure continuing suitability, adequacy, and effectiveness, including governance and management of information security and cybersecurity controls in the organization.

4. IT Security Approach

4.1 **IT Administrators** shall comply with the rules spelled out in IT security regulation and all applicable standards and procedures for safeguarding ThaiBev’s IT assets and resources in their control against theft, loss, and misuse.

4.2 **Users** shall comply with the rules, standards, and procedures for users defined in IT security regulation for safeguarding any ThaiBev’s IT assets and resources in their use against theft, loss, and misuse.

5. Escalation Process

Queries and/or concerns with security breaches and/or vulnerabilities should be escalated to the Management or CIO.