CENTRALRETAIL

Information Security Mission Statement and Policy

Central Retail Corporation Public Company Limited

26 June 2025

Information Security Mission Statement and Policy

Central Retail Corporation Public Company Limited (the "Company") recognizes the importance of corporate management to drive business expansion, stable financial position and generate appropriate returns to shareholders, as well as compliance with good corporate governance principles and the principles of auditing and balancing in the current competitive environment that the Company faces, which has changed over time, either by external or internal factors affecting the Company's competence to fulfill mission and to meet the goals set.

To ensure that the Company can meet the standards of protection expected by customers, shareholders and stakeholders. The Company has adopted international standards such as ISO 27001, NIST, CSF and CIS as part of our hybrid information security program in order to manage the risks and data protection and the Company's core systems. Therefore, the Company has established the information security mission statement and policy.

1. Definition

1.1 "**Data**" means information including general personal data and sensitive personal data.

1.2 "**Sensitive Personal Data**" means personal data relating to a person's race, ethnicity, political opinion, cult, religious or philosophical beliefs, sexual behaviour, criminal records, health, disability, labour union, genetics, biometric or any data which may affect the person.

1.3 "**Personal Data**" means any information relating to a Person, which enables the identification of such Person, whether directly or indirectly, but not including the information of the deceased Persons in particular

1.4 "**Integrity**" means the integrity of data as it maintained over time and across formats with the preservation of the value of information resources (e.g. fraudulently or unauthorized modification of information).

1.5 "**Availability**" means protecting information resources from unintended disruption (e.g. denial of service)

1.6 "**Subsidiaries**" means subsidiaries in accordance with the definitions set out in the Securities and Exchange Commission Announcement No. 17/2008. Re: Determination of the definition in the notice regarding the issuance and offering of securities (including Amended) of the main business in accordance with the Capital Market Supervisory Board Announcement No. 39/2016 Re: Permission and Authorization for the Offering of Newly Issued Shares (including Amended) that are at present or in the future.

1.7 "**Company**" means Central Retail Corporation Public Company Limited.

1.8 "**Person**" means a natural person.

1.9 "**Company Personnel**" means Director Executives, full-time employees, temporary employees, and contract employees of the Company Subsidiaries

1.10 "**Business Unit**" means the Company's business units, Subsidiaries at present or in the future.

1.11 "**Confidentiality**" means protecting resources and information from unauthorized access (e.g. unintentional disclosure)

2. Information Security Mission Statement and Policy

2.1 The Company considers its information security mission to be a valuable contributor to enhance the stability of the company and its' subsidiaries. Therefore, the Company's information security mission is an important mission of the Company.

2.2 The Company and subsidiaries are to take various actions as follows:

2.2.1 Maintain confidentiality, integrity, and availability of data to ensure that data, personal data and sensitive personal data are protected from unauthorized accessing, tampering, and processing.

2.2.2 Shared responsibility.

(a) Maintaining a good level of information security throughout the group is a benefit and what the Company and subsidiaries need from every personnel.

(b) All personnel are responsible for protecting information resources under their control, such as responsibility for protecting personal data, passwords, and sensitive personal data, and following company protocol. Including protocol development for Business Units and related third-party (such as contractors, suppliers, etc.) to maintain security of data and company's IT systems.

(c) Site Management/Department/Office/ Agency are responsible for maintaining the level of information security to be achieved at least at a "Minimum Safety Standards".

(d) Provide details, manuals or guidelines regarding minimum safety standards set out in the document.

2.2.3 Appoint Company Personnel to be responsible for information security which includes continuous reporting the results of security audit, monitoring and testing.

2.2.4 Risk-based approach to improve protection of the information security system

(a) Manage the up-to-date information environment and continuously improve the information security system throughout the group.

(b) Balance openness and control, as well as costs and benefits.

(c) Categorize data based on risk. The level of protection will be determined by varied levels of risk.

(d) Implement effective information security mitigations with risk-based management.

(e) Monitor cybersecurity risks actively.

2.2.5 Defense in depth

Provide more effective risk reduction by implementing several measures at the following levels (but not limited to):

(a) Network - separation by risk, intrusion detection, anti-denial-of-service, etc.

(b) Server-vulnerability management, physical security, etc.

(c) Endpoints - Endpoint Detection Response (EDR), Virus Protection (AV), vulnerability closure, physical security, etc.

(d) Application System - development standards, vulnerability assessment, penetration tests, etc.

(e) Data - encryption, data loss protection, etc.

(f) Individuals - awareness, conformance, and skills, etc.

Examples of effective protection in depth It is a situation where the user has an intention not to open suspicious email attachments, although EDR/ AV protection is already available at End-Point, Network and at server access level.

2.2.6 Holistic consideration for different stages in data life cycle

Rapid advances in IT have led to a relatively shorter life cycle of IT resources, from creation, deployment to retirement. Protection of IT resources and information should be tied in with different stages in the life cycle. For instance, cybersecurity protection for application systems or other IT resources should be embedded in their respective lifecycles, from acquisitions to disposal.

2.2.7 Incident management

The Company is considered to be of great importance to have effective management of security incidents to

(a) ensure that the Company can effectively reduce fraud while remaining compliant with the law.

(b) Details of SOC (Security Operations Center) to be implemented in alignment with the full internal information security policy. Its' structure supports cybersecurity incident management specifically which included incident reporting, impact containing, promptly responding and recovery. Identification of room for improvement from incident lesson learn is also practiced continuously.

(c) To be able to monitor, mitigate risks and respond to information security incidents and threats appropriately with clear communication with affected stakeholders.

3. Enforcement and Management

3.1 To enhance the awareness of information security responsibility for partners and Company's personnel of each business unit by disseminating information, educating, holding seminars or training on such matters to the Company's personnel regularly.

3.2 Define rights and restrictions on access to the Company's personnel information and access request to be recorded, backed up for a reasonable period or for the period specified by law.

3.3 Monitor and assess the risks of information security of each business unit which aligns with corporate risk management practice. The assessment results are actively reviewed and analyzed by executives to identify effective treatment.

3.4 To achieve the results of this information security policy and mission, the Executive Director or Chief Executive Officer may appoint a particular

responsible person to be head of information security of each business unit, or to have the data security controller responsible for the evaluation who can manage and direct compliance with this policy.

This Information Security Mission Statement and Policy is effective from 26 June 2025 onwards.

-Signed-
(Dr. Prasarn Trairatvorakul)
Chairman
Central Retail Corporation Public Company Limited