CENTRALRETAIL

Information Security Mission Statement and Policy

Central Retail Corporation Public Company Limited

(15 December 2021)

CENTRALRETAIL

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. "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.

1.2. "Company" means Central Retail Corporation Public Company Limited.

1.3. "Person" means a natural person.

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

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

2. Information Security Mission Statement and Policy

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

2.2. The Company is to take various actions as follows:

2.2.1. Maintain confidentiality, accuracy, and availability for purpose.

(a) Confidentiality means protecting resources, information and information from unauthorized access (e.g. unintentional disclosure)

(b) Integrity refers to the integrity of the equipment in connection with the preservation of the function of information resources (e.g. fraudulently or unauthorized copying of information).

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

2.2.2. Shared responsibility.

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

(b) All of Company's personnel are responsible for protecting information resources under their control, such as responsibility for protecting personal data, passwords, and sensitive information, etc.

(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. Risk-based approach to protection

(a) Manage the up-to-date information environment throughout the group by providing equal importance from unnecessary risks, including resources and information for operations.

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

(c) Implement effective information security guidelines to prevent risk, including categorize data into different levels or risk types. The level of protection will be determined by vary level of risk.

2.2.4. 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.

2.2.5. Holistic consideration for different stages in data life cycle.

Rapid advances in IT have led to 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.

2.2.6. 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 and

(b) Details of SOC (Security Operations Center) are structured and to be implemented in the full internal information security policy.

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 at least once (1) a year.

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.

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