Data Privacy and Security Policy

CP ALL Public Company Limited and its subsidiaries (hereinafter referred to as the “Company”) are committed to sustainable business operations with responsibility in appropriate management and rigorous protection of the personal data and privacy of customers in accordance with relevant laws.

1) Personal Data

The Company is dedicated to providing convenient services to every community, creating positive impact on the lives of customers and people in general. The Company aims to create a comprehensive offering of products and services that add value for customers in order to cater to the demands of all customer groups. Thus, the Company needs to collect customer information to better understand consumers and use the information for operational reasons.

The Company is fully aware that protection of customers’ private data is of utmost importance as well as respects customers’ privacy. Therefore, the Company’s objective is to manage customer data with transparency.

The policy on data protection and security covers how data is collected, types of data collected, the Company’s objective in using the data, disclosure of data to third parties, and methods employed by the Company to protect customers’ data. The scope of this policy applies to companies in the CP ALL Group and all contract parties of the CP ALL Group.

How Data Is Collected

The Company collects customers’ personal data as follows:

□ When customers apply to use the services of the CP ALL Group

□ When customers use the services of the CP ALL Group

□ When customers contact the customer service center of the CP ALL Group

□ When customers respond to requests made by the CP ALL Group

□ When customers join various programs and activities of the CP ALL Group

□ When customers use benefits or privileges of loyalty programs of the CP ALL Group such as 7Eleven Card, 7Eleven Member point

Types of Data Collected

The data of customers that the Company collects isgrouped as follows:

- □ Personal data such as name, birth date, personal ID number, address, and information on website use, cookies and how you use information
- □ Information on service use such as purchase information and issue of receipts / tax documents
- □ Information on service use and number used to contact the Company through various channels such as the call center and email, as well as inquiries or services requested by the customer
- □ Information on customer benefits or privileges such as the use of benefits or privileges of the loyalty program, specially priced products and services, and special channels to contact the Company

Use of Data

- □ For internal analysis of the organization's operations such as customer orders and payment, delivery and product service
- □ For market research in order to understand customer needs and wants to design products and services to meet customer demands
- □ To offer new products, rewards, benefits and privileges that are of interest and related to customers

Disclosure of Data to Third Parties

The Company will not disclose your information to any other company, organization or person, except in the following events:

- □ The Company has received permission or consent from you
- □ The disclosure of such information is for the purpose of external assessment and for business partners who provide service to you
- □ The Company is required to disclose such information for legal reasons

Protection of Data

The Company is committed to protect your data with the highest security and applies various standards effectively as follows:

□ Application of strict technical security to protect against illegal use of data

□ Strict limited access to the data system and establishment of strict procedures to authorize right to access data by employees

□ Requirement to sign confidentiality agreement every time before authorizing right to access customer data

□ Create awareness of the importance of data security among personnel at all levels and determine specific personnel who are in charge of the data system

The Company is committed to the highest protection of customer data and has implemented standards to develop and maintain customer data security. The Company has received ISO/IEC 20000 certification (IT service management), ISO/IEC 27001 certification (information security management system), and PCI DSS certification (Payment Card Industry Data Security Standard). All three standards are internally and externally reviewed to ensure customers of the Company's effective system and to provide confidence that customer data is protected by the CP ALL Group.

Respect for Customer Privacy

The Company gives utmost importance to respect for customer privacy. Customers may choose not to receive any marketing information from all channels of communication. After the customer chooses not to receive any marketing information, the customer will still continue to receive information related to services such as service alerts.

2) Data Security

The Company is committed to the highest quality of Information Security Management (ISM) and strictly adheres to ISO/IEC 27001, ISO/IEC 20000, and PCI DSS, under the supervision of the Risk Management Steering Committee. The Chairman and Members of the Risk Management Steering Committee include executives who oversee Information Technology Operations and Information Technology Security.

The Company has a data security policy that ensures that the Company's business operations and customer service is effective. There are 10 main policies which cover customers, contractors, business partners, service providers and companies in the Group as follows:

1. Information Security Management Structure There is a unit responsible for information security management that determines measures to promote information security for the whole Group.
2. Information Resource Management Classification of information resources that should be protected; rank the importance of each resource; and appropriate management according the information resource record format.
3. Management Information Systems Implement the following measures to all information systems that use information resources to ensure thatanalysis of the information is correct, accurate and secure
    (1) Network management
    (2) System management
    (3) Information management
    (4) Deficiency management
    (5) Change management
    (6) Log management
4. Management of Physical EnvironmentThe Company stores data in its own computer center with area management according to classification and importance to ensure that information resources are under appropriate control.
5. Human Resource Management Establishprocedures for training, to learn about and use the information system and to adhere to the regulations relating to information resources and data security as well as this policy in a strict manner, to ensure that executives, employees, part-time staff and all persons who use the Company's information resources perform their duties with understanding of the rules for data use and are aware of the responsibility for data security prior to employment until termination of employment, and to develop IT system personnel to have expertise and be up-to-date on new cyber threats.
6. Outsourcing In hiring external companies that relate to the use of information resources, there must be control through contracts and confidentiality agreements and cleardetermination of the scope of responsibilitiesthat the service provider must strictly comply with, in order to protect the Company's information resources.
7. Compliance The Company has established measures relating to the correct and legal use of information resources and strictly adheres to the laws of each country in order to avoid any wrongdoing related to security, contracts, and laws and regulations on information security.

8. Management of Cyber ThreatsEstablish plans and infrastructure to deal with cyber threats in order to overcome cyber threats that might affect information security as well as inform of all security incidents such as information leak from virus, phishing and cyber attacks, in an effective and regular manner.
9. Business Continuity Management Establish measures for business continuity including data backup, designed system ready for use and to serve customers, preparation of plans, drills, and procedures for business continuity reporting in the event of disasters to ensure effective systematic implementation and quick and efficient return to normal operations.
10. Evaluation and Review The Company has regular evaluation and review from both internal and external auditors to assess the status and security of data, whether security is appropriate or needs to be enhanced in order to reduce risks, and to plan for improvement of information security management.

Protecting the security of customers' private data by keeping it confidential and not disclosing the information without authorization is the priority of all employees. There are penal measures according to the employment regulations for employees who do not comply with the policy.