Cybersecurity and Privacy Protection

The linkage between the Company's operating data and personal information has innovatively been transformed into Digital Transformation and the Internet of Things (IoT). In addition, due to the Company's retail business having to deal with a large number of agencies, including business partners and customers, each day, information is collected and added into the digital network. This large volume of transfers of information has made the Company conscious of cybersecurity and the stability of the information network that may face the risks of cybercrimes, which are currently becoming more violent. If business data is stolen by a cyberattack or a customer's personal information is leaked due to a system failure, it will have a serious impact on the economic, social, security, and reliability dimensions of shareholders and customers. The Company realizes the importance of compliance with the law and having strict cybersecurity and data privacy management policies to help reduce the risk of cyber espionage and its potential impact.

Cybersecurity

The company is committed to maintaining a secure and strong internal digital technology network that is strong against cyber espionage to prevent the leakage of confidential information related to the management of the company due to system errors. The Company has established an IT agency, which is a network security agency made up of to supervise the system by establishing guidelines for the storage and transfer of information in the information system within the company, including the management of the physical security system of the computer center, which strictly controls the access of personnel, as well as the operating process of security for the use of digital technology in data management. The Company's business operations are as follows:

Cybersecurity Process

Working Committee	Organize monthly SCM (Security Committee Meeting) between departments of safety supervision attended by Cyber and IT executives of each sub-business group.
Steps	Stay updated and exchange information on cybersecurity, risk and data privacy. Process to find methods of risk assessment.
Cyber Security Framework	Improve methods and establish a framework for practice. Including preventive technology systems in accordance with CIS Control and NIST CSF.

Data Privacy Protection

The Company realizes the importance of protecting the personal information of customers that have been collected, used, disclosed, and transferred for use in receiving services and purchasing products. The information collected is intended to be used to customize recommendations for customers. The Company is committed to taking responsibility and protecting personal information of all stakeholders, including shareholders, employees, customers and business partners. Therefore, the Company has published its privacy policy on the website related to the subsidiary company group to show the transparency of its operations. This is managed under the department that is responsible for protecting personal information of customers, for which the operating framework is consistent with Personal Data Protection Act (PDPA). The Privacy Policy covers the use of information in stores, service through all online channels, and the customer service call center (operating under the Company). Details are as follows:

- Type of personal information
- Purposes for Collection, Use and Disclosure of Information
- Agencies or individuals that the company may disclose
- Transfer of information abroad
- Personal Information Storage Timespan
- Information security
- Cookie Policy
- Rights of the Personal Information Subject
- Contact Channels regarding the right to personal information

Contact and Complaint Regarding Privacy and Personal Information Offenses

The Company has provided channels for customers and shareholders to inquire about personal information or express the intention to exercise the right to access the information collected by the company, including making complaints of privacy and personal information violations through the channels announced in accordance with the following privacy policy.

CENTRALRETAIL

Contact channels

Central Retail Corporation Public Company Limited

Central Chidlom Tower, 14th Floor, 22 Soi Somkid, Ploenchit Road, Lumpini Subdistrict, Pathumwan District, Bangkok 10330

Call Center: +66 2 650 3600, +66 2 730 7777

Email: pr@central.co.th, contact@central.co.th

Performance

In the past year, the Company has collected a number of reports and complaints related to privacy and personal information offenses where data have been leaked to unrelated persons, which the results are as follows:

Cases of Complaints	2019	2020
Complaints directly from customers or third parties about privacy offenses committed by the Personal Data Protection Officer.	0	0
Complaints from government agencies regarding breach of customer privacy.	0	0
Number of times customer data is leaked from cyberattacks.	0	0

The Company takes action regarding complaints of personal information breaches through the Personal Information Review Committee. The cause of the complaint will be investigated and the Company will take action as quickly as possible since it is required by the law to protect the privacy of its customer. In addition, if found that the personal data breach has an impact on the complainant's rights and freedoms arising from the work of the employees, the Company will continue to report the infringement and offer remedies as appropriate.