

Achieving Governance

President Chain Store Corporation abides by the principle of ethical corporate management from its internal operations to its external value chain to ensure long-lasting and stable operations. In the meantime, President Chain Store Corporation identifies and stays updated with the trends in regulatory revisions, as well as ensuring all operations of the Company's organizations comply with government laws and regulations to uphold the rights and interests of consumers and the Company. Risk management is the key to sustainable operations. To this end, we have set up a dedicated unit for cross-departmental communications to avoid negative impacts and increase the value of the Company. In addition, we attach importance to the management and protection of customer privacy, as well as providing better services based on data generated from customer purchasing behavior.

Sustainable Development Goals & Management Policies



SDG 8 Decent Work and Economic Growth

- Annual consolidated revenue reached a record high of **NT\$350,734,591** thousand



SDG 16 Peace, Justice and Strong Institutions

- The Integrity, Risk and Cybersecurity Management Committee operates at the Board level, comprehensively strengthening information security control



SDG 12 Responsible Consumption and Production

- Zero information security incidents occurred
- The invoice systems of all stores and uniopen membership passed ISO 27001 Information Security Management System certification

Corresponding Material Topics

- Information Security

Policies and Commitments

- Data Protection Management System and Policy
- President Chain Store Corporation Personal Information File Security Maintenance Plan ([Personal Data Protection Handbook](#))
- [President Chain Store Corporation Risk Management Policy](#)
- [Articles of Incorporation](#)

Management Actions

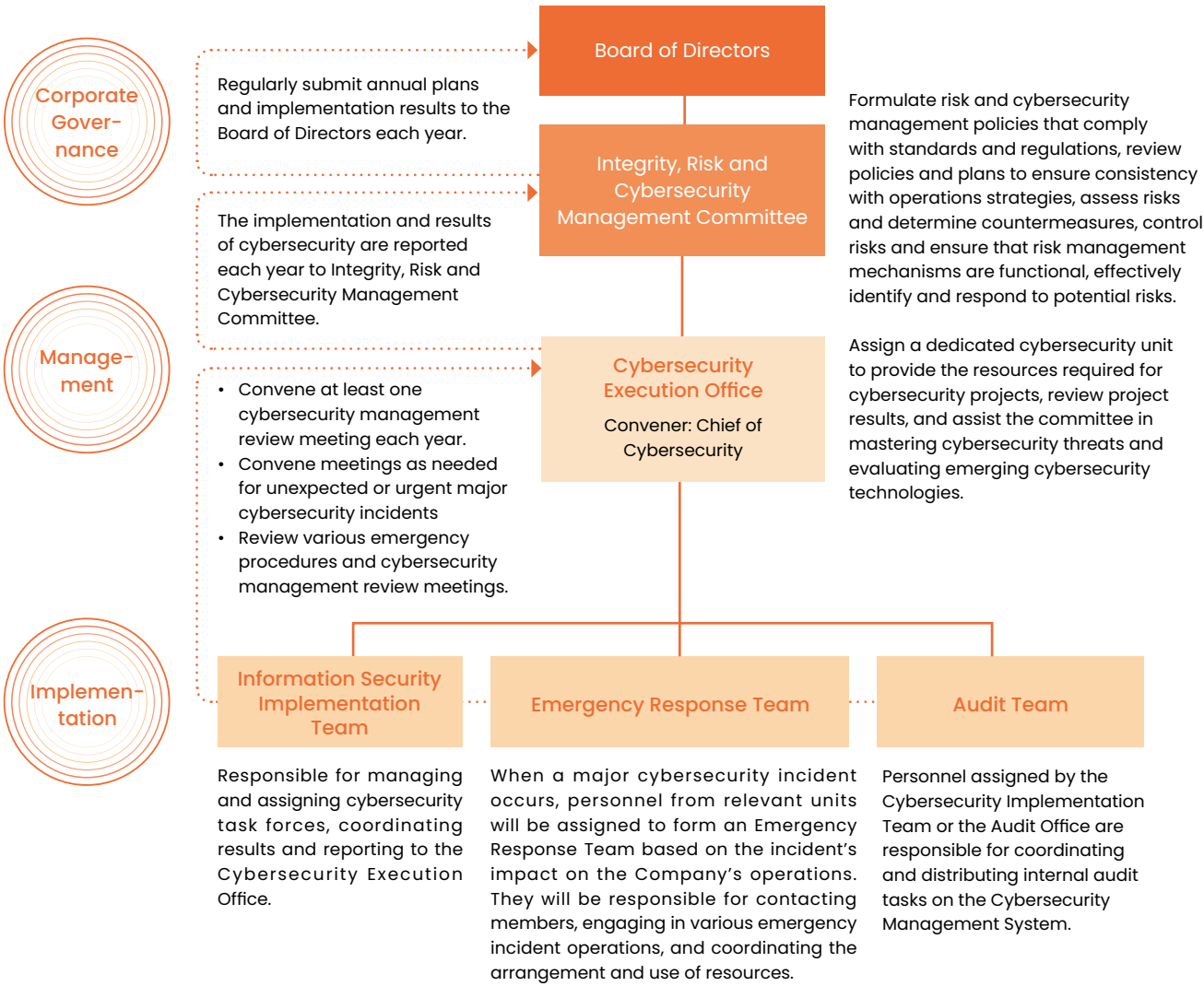
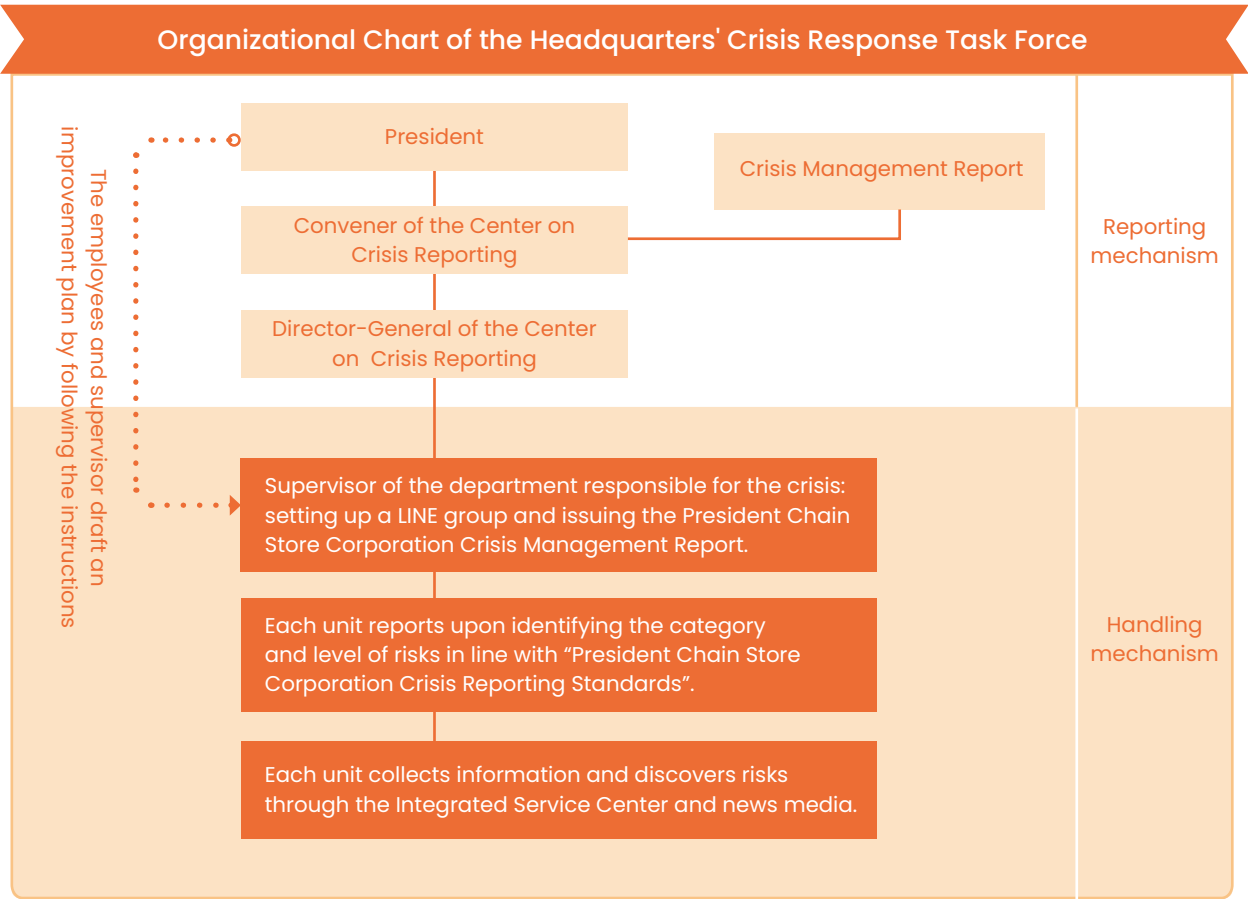
- President Chain Store Corporation has set up a Personal Data Protection Task Force to ensure the safety of consumer data through internal audits and external verification of personal data (Taiwan Personal Data Protection and Administration System, TPIPAS), crisis prevention and education and training.
- In November 2023, President Chain Store Corporation's Board of Directors resolved to set up the Risk & Cybersecurity Management Committee. On July 30, 2025, the organization was renamed the Integrity, Risk and Cybersecurity Management Committee to strengthen information security control and manage risks more comprehensively.

Sustainable Goal Management Process

Material Topic	Management Metrics	Medium- and long-term Targets	2026 Targets	2025 Targets & Performance
Information Security	(1) Number of information leakages (2) Proportion of information leakages containing identifiable personal information (3) Number of customers affected by information leakages (4) Number of violations that infringe on customer privacy and total fines paid due to information security incidents	By 2028 (1) ≤ 1 (2) $\leq 30\%$ (3) ≤ 600 records (4) $\leq 700,000$	(1) ≤ 2 (2) $\leq 40\%$ (3) ≤ 800 records (4) $\leq 800,000$	(1) ≤ 3 (2) $\leq 45\%$ (3) ≤ 850 records (4) $\leq 850,000$ No such incidents occurred

↑ Exceeded ✓ Achieved — Not Achieved

All departments involved will set up a review team (LINE group) for the crisis for prompt response and discussion. Subsequently, all departments involved will make improvements and provide responses to the crisis to avoid recurrence. We review the crisis management process with strict mechanisms to consolidate the operations of President Chain Store Corporation from occurrence, handling to external response to crisis events.



2.3 Information Security and Privacy Protection

President Chain Store Corporation takes advantage of the power of digital technology to make consumers' lives more convenient. To this end, it provides customers with cash flow, logistics and information flow services with digital tools such as the 7-ELEVEN online shopping site, uniopen, ibon, OPEN Wallet, icash Pay, icash 2.0, OPENPOINT app (including iGroupbuying® and iPre-order) and MyShip. This allows consumers to make the most of President Chain Store Corporation as the base and service center for everything in life.

· Cybersecurity Execution Office ·

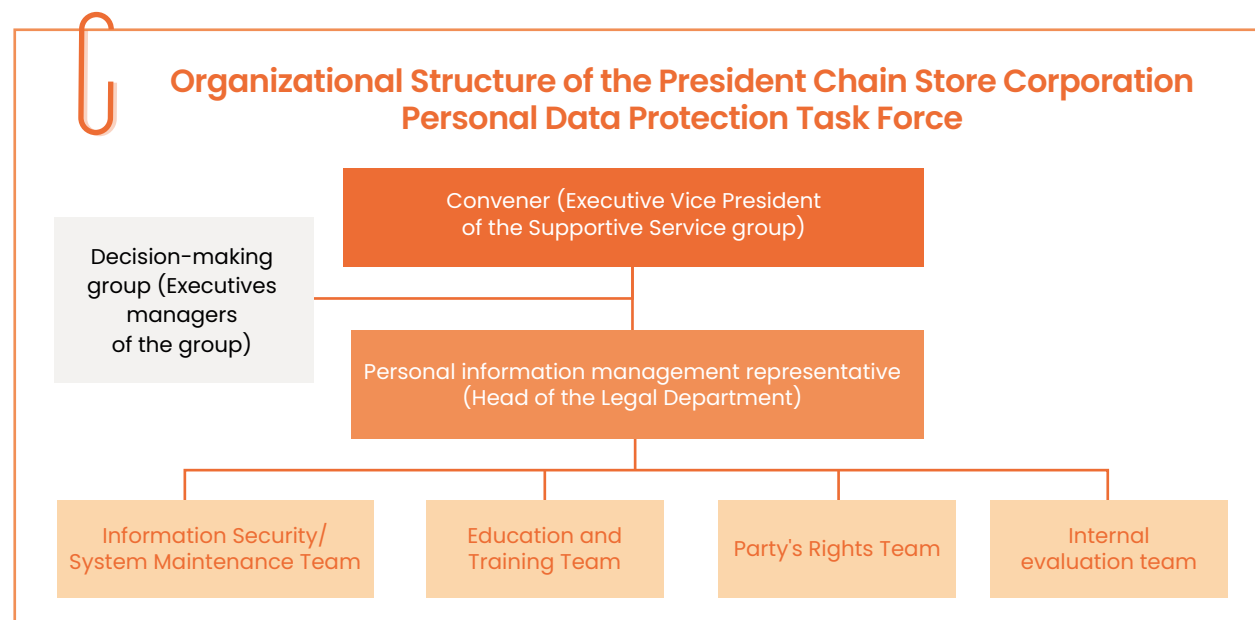
The "Cybersecurity Execution Office" is the highest decision-making unit for President Chain Store Corporation's information security management. It was originally under the "Sustainable Development Committee," and moved under the "Integrity, Risk and Cybersecurity Management Committee" in 2023. Previously known as the Cybersecurity Committee, it was renamed as the Cybersecurity Execution Office in December 2024. Chaired by the Chief Information Security Officer, the Office oversees the "Information Security Implementation Team," "Emergency Response Team," and "Audit Team," and convenes at least one review meeting annually, with the convener regularly reporting the implementation and results of information security implementation to the Risk and Cybersecurity Management Committee ^(Note).

Note : The policies, specific management plans and resources invested by the Cybersecurity Execution Office can be obtained from [the Company website](#).

· Personal Data Protection Task Force ·

President Chain Store Corporation uses customer data for non-primary collection purposes, which include marketing or communications with customers in compliance with laws and with the consent of customers. We comply with relevant government regulations and information management principles to ensure that the collection and use of data must be within the scope of authorized data established by the Company, adopt appropriate technical and organizational security measures, and preserve data strictly in highly secure and stable data storage systems to fulfill the confidentiality obligations of personal data of customers and investors. In 2025, the proportion of customer personal data used by the Company for marketing and communications accounted for 99.5%. Digital technologies involve a lot of customers' personal data. President Chain Store Corporation has established a special task force and reporting mechanism, and conducts training and internal audits to ensure the protection of consumers' personal data.

The "Personal Data Protection Task Force" is an cross-departmental task force that regularly performs personal data inventory, risk analysis, internal system review, notification and revision, data destruction, education and training. Education and training is systemized with courses and forums for new employees and personal data liaisons of each unit to complete via testing, achieving a 100% internal training completion rate. In order to enhance the awareness and expertise of all employees regarding cybersecurity, we regularly publish cybersecurity e-newsletters to share the latest trends in cybersecurity, information on threat and protective measures. In the meantime, all subsidiaries and system contractors' IT personnel are required to complete 3 hours of cybersecurity education and training every year. In addition to integrating personal data risk management into the overall risk management and audit mechanism of the Company, personal data protection management reports are formulated for each department, as well as adding personal data protection clauses to contracts when working with external suppliers to ensure that all operating units and suppliers comply with the Company's personal data protection policy. President Chain Store Corporation's internal evaluation plan and external verification system can effectively supervise and assist various departments in formulating corrective, preventive or improvement measures for non-conformities discovered during internal evaluations or audits. Records of improvement are equally made and kept. Corresponding penalties are also formulated for employees who violate the Company's personal data management rules. Any violation will be reported to the supervisor and included in the employee's personal performance evaluation and records.



The above figure presents the organizational structure for 2025. The working group adjusted the organizational structure effective April 1, 2026.

Internal Audit and External Certification

President Chain Store Corporation integrates information security management and control into the overall risk management and auditing mechanism of the enterprise, and further links the annual performance evaluation of employees. Through the internal assessment and external verification system, it can effectively identify risks and supervise various departments in formulating corrective and preventive measures for non-compliance matters to achieve continuous improvement. For critical information and communication systems, a business continuity plan or regular testing plan ^(Note) should be conducted at least once a year. In addition to checking the settings of operating systems and network services and evaluating account and password management principles, testing will also cover other related areas to identify vulnerabilities in the information and communication environment. For overall information and communication protection, red team drills are performed to identify the vulnerabilities, as well as immediately implementing management and technical strengthening measures based on the result to ensure that the security of the information and communication systems meets the requirements of international common standards and best practices.

Note: Business continuity/regular testing plan include vulnerability scanning and penetration testing, business continuity drills, social engineering drills and red team drills.

Note : Detailed cybersecurity test results can be accessed on [President Chain Store Corporation's website](#).



President Chain Store Corporation first obtained certification under the Taiwan Personal Information Protection and Administration System (TPIPAS) in 2014, and received renewed certification valid for two years in 2023. In addition to this personal data protection certification, the Company passed renewed certification for the ISO 27001:2022 Information Security Management System in 2025, covering the electronic invoice systems of all stores and uniopen membership, thereby strengthening its information security management mechanism. In addition, we undergo external audits each year. The 2025 audit was completed on November 7, 2025, with no nonconformities identified, and the certificate is valid until January 10, 2029. In accordance with ISO 27001:2022 requirements, we also conduct supplier audits twice a year. For high-risk contractors identified by the Company, we regularly assess preventive measures for potential risks such as information security vulnerabilities, data breaches, and privacy compliance.

Based on the above certifications, the Company further implements the principle of Privacy by Design in the development processes for products, services, and systems. This covers data minimization, restrictions on use for specified purposes, and default protection measures. Personal data review procedures are also established at each stage of development, including determination of personal data involvement at the requirements stage, data flow analysis at the design stage, and personal data and information security risk assessments before launch, ensuring that privacy protection runs through the entire development lifecycle.

Stage	Key Actions	Document Output
Applicability Determination	Confirm whether President Information Corp. is responsible for the entire process, from planning, design, and construction to operations and maintenance	
Requirements Stage	BIF Determine whether personal data is involved ► identify personal data and prepare the BIF	BIF Enterprise Information Flow Overview Diagram
Design Stage	Conduct data flow analysis and confirm the five major assessment items	Data Flow Analysis Document
Pre-launch Review	Major / controlled projects must complete personal data and information security risk assessments	Risk Assessment Report; PMP006 CheckList
Operations and Maintenance Management	regular spot checks ► improve deficiencies when identified ► continue the cycle	Spot Check Records; Improvement Reports

Grievance Mechanism

To provide customers with comprehensive personal data protection, President Chain Store Corporation has also set up personal data issue reporting and contacts that correspond to our various personal data collection channels. In 2025, no complaint was received regarding customer privacy infringement from the competent authority or external parties.

Personal Data Grievance and Contact	
Consumer	Integrated Services Center Tel : 0800-008711 E-mail : public@mail.7-11.com.tw All President Chain Store Corporation departments have respective contact persons for reporting privacy issues.
Non-consumer	As there are many departments within President Chain Store Corporation, it is impossible to list every point of contact for reporting privacy issues. These points of contact are also responsible for handling and responding to privacy issues. The processed cases will be reported to the Personal Data Task Force for record-keeping.