Confidentiality level: Secret

President Chain Store Corporation

Information Security Management Policy

May 22nd, 2025

Article 1 Purpose

The purpose of establishing this information security management policy of President Chain Store Corporation (hereinafter as the "Company") is to reduce the risk of the improper use, leakage, tampering or destruction of the Company's information assets (included network equipment, computer devices, application systems, human resource security and Supplier Relationships) caused by factors such as human negligence or natural disasters and further ensure the Company achieves its information security objectives. The Company's information security objectives are:

1. Confidentiality: To ensure that only authorized users can access information.
2. Integrity: To ensure the accuracy and completeness of information and information processing methods.
3. Availability: To ensure that authorized users can timely access information and related assets when needed.

This policy declares the Company's support for mitigating information security management risks, improve information security management system, and protecting the benefits of the Company and custormers.

Article 2 Scope

All employees of the company and third-party external personnel.

Article 3 Definition

None.

Article 4 Policy

1. **Information Security Management System(ISMS)**

(1) General

The Company shall establish, document, implement and maintain the ISMS based on the requirements of ISO/IEC 27001 to maintain the effectiveness of the ISMS and protect the Company’ s information and informatioin systems.

(2) Operation

The Company adopts the Plan-Do-Check-Act (PDCA) cycle operation model based on ISO/IEC 27001 to establish and implement the ISMS and maintain its effective operation and continuous improvement.

A. Planning and establishment (Plan): Based on the company's overall strategy and goals, establish an information security management organization to control potential threats and vulnerabilities, plan risk assessment, design and build processes and controls to establish the ISMS.

B. Implementation and operation (Do): Based on the results of Plan, establish or modify the appropriate processes and controls.

C. Monitoring and Audit (Check): Monitor the implementation of information security processes and controls. Evaluate and audit the effectiveness of information security processes and controls.

D. Maintenance and Improvement (Act): Based on the results and recommendations of the monitoring and audit, implement corrective actions to continuously improve the information security processes and controls.

2. Responsibilities

(1) An information security management organization should be established to be responsible for promoting, coordinating and supervising the following about ISMS:

A. Development, review, promotion and supervision of information security policies.

B. Assignment and coordination of information security responsibilities.

C. Promote the responsibility to comply with information security goals, information security policies, and regulations, as well as the need for continuous improvement.

D. Provide sufficient resources to establish, implement, operate, monitor, review, maintain and improve the ISMS.

E. Develop criteria for risk acceptance criteria.

F. Develop information security audit plans, information risk assessments and irregular information security testings.

G. Organize the ISMS management review issues and materials.

H. Identify the internal and external interested parties of the ISMS, consider their needs and expectations, and determine the required internal and external communication.

I. Review and supervise information security incidents and consider internal and external issues that may affect the ISMS.

J. Implement information security-related education or training every year, and evaluate the effectiveness of the information security education or training provided.

K. Approval of other information security matters.

(2) Management Review

The company's management review is carried out by the

Cybersecurity Execution Office once a year to continuously ensure that the operation of the ISMS is appropriate, sufficient and effective. The scope of the review includes the ISMS improvement plan and change requirements. The result of management review should be recorded in detail and properly kept.

(3) Information security monitoring and measurement indicators

The Company should establish Information security monitoring and measurement indicators to evaluate the performance of the ISMS. Information security monitoring and measurement indicators should at least include information such as measurement items, methods, time, frequency, and responsible personnel. Information security monitoring and measurement indicators should be appropriately integrated with the Company’ s information security policy.

(4) Internal Audits

Internal audits should be conducted regularly or irregularly to review whether objectives, processes and controls are in compliance with relevant standards, laws and regulations or information security requirements to continuously improve the ISMS.

(5) Personnel Safety Management

A. All employees of the company must comply with the Personal Data Protection Act and the regulations of "Personal Data Project - Data Reporting for Each Department" enacted by each department.

B. Regularly provide employees with appropriate information or training on information security in order to enhance their safety awareness and understanding of the correct operation

of computer equipment and the use of information.

(6) Management Requirements for Third Parties

A. Vendors that need to use the company's information resources must have antivirus software installed on their information equipment, with real-time updates of virus definitions and scanning engines configured, before it can be used within the company.

B. If vendors need to use the network services provided by the company, they must comply with the "Network Usage Management Regulations." Accessing any form of company files or data without the company's consent is prohibited. In the event of data theft or information security breaches, legal action will be taken, and the vendor will be held liable for compensation.

C. The contractual terms of the vendor, if involving the borrowing of company information resources, must be evaluated by the information security management unit to ensure there are no information security concerns before being finalized.

(7) Continual improvement of the ISMS

A. The Company should continue to improve the effectiveness of the ISMS through internal and external audits, information security incident analysis, corrective actions, and management reviews.

B. Corrective actions

The Company shall implement appropriate actions to reduce nonconformity discovered during the operation of the ISMS and prevent their recurrence. The procedures for corrective actions are as following:

- Identify various nonconformity.

- Root cause analysis.
- Evaluate the actions that need to be taken.
- Determine and implement necessary corrective actions.
- Document and review the effectiveness of corrective actions taken.

(8) Document management system

A. Document management

The management, issurance and change of the Company's ISMS document shall be handled in accordance with the Company's document management procedures.

B. Records management

Any documents, forms and records generated by the operation of the Company's ISMS should be properly kept by designated record keeping personnel to facilitate tracking the execution status of the ISMS.

(9) Policy review

This policy is reviewed at least once a year to meet the needs and expectations of internal and external interested parties.

(10) Compliance

All employees of the Company must abide by this policy. Violators must be punished in accordance with the relevant regulations of the company. If there are relevant criminal or legal liabilities, such as business secrets law, copyright law, personal data protection law, etc., the Company’ s shall reserve the right to take legal actions.

3. Information security management principles

The principles shall include, but not limited to, the following:

A. Information Security Organization

B. Human resources security
C. Asset Management
D. Access control
E. Cryptography
F. Physical and Environmental Security
G. Operational safety
H. Communication security
I. System acquisition, development and maintenance
J. Configuration management
K. Cloud service management
L. Supplier management
M. Threat Intelligence Management
N. Information security incident management
O. Operational continuity management
P. Compliance

Article 5 Reference

None.

Article 6 Approval and revision

This policy shall be implemented after approval by the board of directors.