Risk Management Policy and Procedure

of

President Chain Store Corporation

July 30th, 2020

Amended on August 4th, 2022

Amended on December 14th, 2022

Amended on November 1st, 2023

Amended on December 19th, 2024

Amended on July 30th, 2025

Article 1 Purpose

To improve risk management policy of President Chain Store Corporation (hereinafter as the "Company") and achieve sustainable development goals under prudent operation, the Company hereby establishes this Risk Management Policy and Procedure (hereinafter as the "Policy") according to the international standard 'ISO 31000 Risk Management – Principles and Guidelines' and in compliance with Article 44 of the 'Regulations Governing Establishment of Internal Control Systems by Public Companies' issued by the Financial Supervisory Commission, as well as the 'Risk Management Best-Practice Principles for Taiwan Stock Exchange and Taipei Exchange listed Companies' jointly issued by the Taiwan Stock Exchange Corporation and the Taipei Exchange.

Article 2 Scope of Application

The Company endeavors to maintain comprehensiveness of the Policy, and has listed the Company, its affiliates and subsidiaries within the scope of management. The Policy will apply to any and all levels of risk management operation.

Article 3 Target

In order to reach following targets, the Policy is aimed to control various risks that may affect business operation through risk management system and integrate risk management system into operation activity and daily management

1. Reach business goals.
2. Improve operation and management efficiency.

3. Effectively and appropriately redirect the resources

Article 4 Scope

4.1 Scope of the Policy includes but not limited to operational risk, market risk, financial risk, compliance risk, climate risk and other risks that may cause significant losses to the Company. Each department shall implement the Policy according to issues under its responsibility, and continues to pay attention to international and domestic risk management, promptly identify new type of risks.

4.2 Consideration the Company's scale, business features, risk nature, and operating activities, the Company develops a sound risk governance and management structure where risk management is linked to the Company's strategy and goals through the participation of the Board of Directors, functional committees, and senior management. In this way, the Company's material risk items are identified, the results of risk identification become more comprehensive, perspective oriented, and complete, and corresponding risk control and measures are promoted and initiated in a top-down manner, to ensure reasonably accomplishment of the Company's strategic and goals.

4.3 The Company promotes a top-down risk management culture. Awareness of risk management is integrated into day-to-day decision making and a comprehensive corporate risk management culture is fostered through express risk management representations and undertakings of the governance unit and senior management, the establishment and support of a risk management unit, and the offer of professional risk management training across the levels.

4.4 The Company offers sufficient resources and support, integrates the responsibilities of various units within the Company, and promotes communication, coordination, and collaboration between units to drive the implementation of risk management across the organization, ensuring its effective operation.

Article 5 Risk Management Execution Office & Responsibility

5.1 Integrity, Risk, and Cybersecurity Management Committee is subordinate to the Board of Directors. The Board serves as the highest authority for risk management within the Company and has established the Integrity, Risk, and Cybersecurity Management Committee under its supervision. The Committee is comprised of all

independent directors, and the Chairperson is elected by and from among its members.

5.2 Integrity, Risk, and Cybersecurity Management Committee consists of Risk Management Execution Office, Cybersecurity Execution Office and Integrity Management Promotion Team. Risk Management Execution Office integrates and manages strategic, operational, and financial risks etc. that may affect operations and profitability of the Company, and actively communicates with risk-related stakeholders of the Company to reduce the impact on the Company's operations when risk events occur. Organizational responsibilities are described as follows:

5.2.1 Board of Directors:

(a) Ensure consistency between the direction of operational strategy and the risk management policy;

(b) Ensure an appropriate risk management mechanism and risk management culture have been established;

(c) Oversee and ensure effective operation of the entire risk management mechanism;

(d) Allocate and designate adequate and appropriate resources for effective operations of risk management.

5.2.2 Integrity, Risk, and Cybersecurity Management Committee:

(a) Examine the risk management policy, procedures, and structure, and review their applicability and the effectiveness of their enforcement on a regular basis;

(b) Approve the risk appetite (risk tolerance) to facilitate allocation of resources;

(c) Ensure the risk management mechanism is able to address adequately risks faced by the Company and incorporate the mechanism into day-to-day operating procedures;

(d) Determine the priority order and risk level of risk control;

(e) Examine the enforcement of risk management, propose necessary recommendations for improvement, and report to the Board of Directors on a regular basis (at least once a year);

(f) Enforce the risk management policy of the Board of Directors.

(g) Promoting and overseeing the implementation of the ethical business policy and prevention programs.

5.2.3 Risk Management Execution Office:

(a) Draft the risk management policy, procedures, and structure;

(b) Draw up the risk appetite (risk tolerance) and develop qualitative and quantitative metrics;

(c) Analyze and identify sources and types of Company's risks and review the relevant applicability on a regular basis;

(d) Compile and present a company risk management enforcement report on a regular basis (at least twice a year);

(e) Assist with and oversee the conduct of each department's risk management activities;

(f) Coordinate interdepartmental interaction and communication in regard to risk management;

(g) Enforce the risk management policy of the Integrity, Risk, and Cybersecurity Management Committee;

(h) Plan risk management training programs to enhance overall risk awareness and culture.

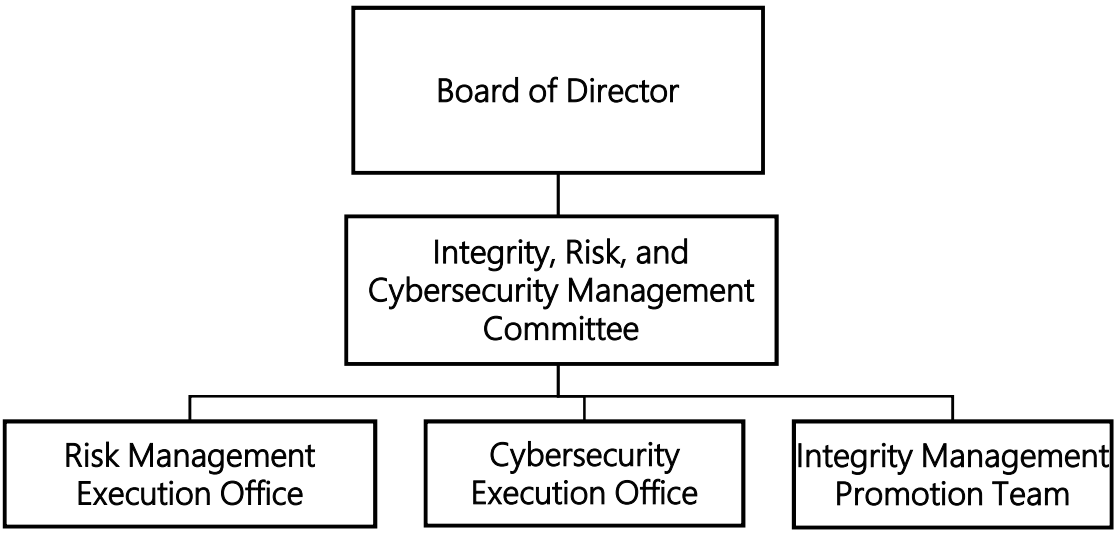
5.2.4 Task Force

(a) Responsible for identification, analysis, and assessment of, and response to, risks of the unit to which it belongs, and create the relevant crisis management mechanism where necessary;

(b) Present risk management report to the Risk Management Execution Office on a regular basis;

(c) Ensure effective enforcement of risk management and relevant control procedures of the unit to which it belongs, to ensure compliance with the risk management policy.

Organizational chart:



Article 6 Risk Management Procedures

Risk Management Execution Office identifies, analyzes, measures, monitors, responds to, reports in accordance with characters of risks and impact levels replied by each department, and improves corresponding measures. The procedures are as follows:

6.1 Identify

6.1.1 Each Task Force shall perform risk identification in respect of the short-, mid-, and long-term goals and business functions of the unit to which it belongs, in accordance with the strategic goals of the Company and the risk management policy and procedures approved by the Board of Directors.

6.1.2 Utilize various practical analytical tools and methods to effectively perform risk identification, and that to perform based on previous experience and information and taking into account internal and external risk factors and stakeholders' primary concerns, to conduct analyses and discussions in a "bottom-up" and "top-down" approach, and integrate strategic risks and operational risk, in order to identify all potential risk events which may prevent the accomplishment of Company goals, occasion losses to the Company, or cause a negative impact on the Company.

6.2 Analyze and Measure

6.2.1 Risk analysis is mainly to ascertain the nature and features of a risk event which has been identified. Each Task Force shall analyze the probability and degree of impact of any risk event which has been identified, taking into account the comprehensiveness of current relevant control measures, previous experience, and cases in the industry etc., in order to calculate the risk value.

6.2.2 The Risk Management Execution Office develops appropriate quantitative or qualitative metrics based on the Company's risk features as the basis for risk analysis. Qualitative metrics express the probability of occurrence and degree of impact of a risk event through textual description; quantitative metrics express these aspects through specific measurable numbers such as days, percentages, amounts, people, etc.

6.2.3 The Risk Management Execution Office draws up a risk appetite (risk tolerance) and submit it to the Integrity, Risk, and Cybersecurity Management Committee for approval in order to determine the risk limit acceptable to the Company. And based on the risk appetite, determine the corresponding risk levels for each risk

value and the risk response methods for each level, serving as the basis for subsequent risk evaluation and risk response actions.

6.2.4 The purposes of risk evaluation are to provide the Company with a basis for decision making, whereby risk events which shall be addressed on a priority basis are determined through a comparison of the results of risk analysis to the risk appetite, and to serve as reference for subsequent formulation of response options.

6.2.5 A Task Force shall devise and enforce risk response proposals by the level of risk based on the results of risk analysis vis-a-vis the risk appetite approved by the Integrity, Risk, and Cybersecurity Management Committee.

6.2.6 Results of risk analyses and evaluation shall be documented accurately and reported to the Integrity, Risk, and Cybersecurity Management Committee for approval.

6.3 Monitor and Response

6.3.1 Risk response plans shall be devised, their full understanding and enforcement by relevant personnel ensured, and their enforcement overseen on an ongoing basis.

6.3.2 The Company shall take into account its strategic goals, the perspectives of its internal and external stakeholders, its risk appetite, and the resources available in selecting the risk response(s) to adopt to make such risk response proposal strike a balance between the accomplishment of the goal and the cost-effectiveness.

6.4 Report

Summarize the risk management and regularly submit reports to the Integrity, Risk, and Cybersecurity Management Committee and the Board of Directors.

6.5 Oversight and Examination

6.5.1 A risk oversight and examination mechanism shall be expressly defined in the risk management procedures to ascertain whether risk management processes and relevant risk measures continue to operate effectively and incorporate the results of examination in performance reviews and reports.

6.5.2 Risk management shall be lined up with critical processes of the organization to oversee and enhance the benefits of implementation of risk management effectively.

6.5.3 The Company's risk management framework and control processes are established in accordance with the "three lines of defense" model, the internal audit unit serves as the third line of defense, responsible for evaluating the effectiveness of the policies and procedures of the internal control system. Regular audits (at least once every two years) are conducted on the Risk Management Execution Office to ensure the effectiveness of risk control.

Article 7 Report and Disclosure of Risk Information

7.1 Risk Management Execution Office should compile risk information and regularly submit report to Integrity, Risk, and Cybersecurity Management Committee and the Board of Directors.

7.2 The procedures and results of risk management, including risk identification, risk analysis, risk evaluation, risk response measures, relevant information sources, and results of risk evaluation, etc., shall be documented, examined, reported, and properly retained for reference through appropriate mechanisms.

7.3 Risk reporting is advisable that different stakeholders and their specific information needs and requirements, the frequency and time-sensitive of reporting, methods of reporting, and relevance of information to the goals and decision-making of the organization be taken into account in assisting senior management and the governance unit in making relevant risk decisions and performing their risk management duties.

7.4 In addition to disclosing relevant information pursuant to regulations of competent authority, it is also appropriate for the Company to disclose risk management related information in annual reports, sustainability reports, and company websites. Disclosing information shall be include as follows:

7.4.1 Risk management policies and procedures.

7.4.2 Risk management committee organization.

7.4.3 Risk management operations and implementation, including the frequency of report to the Board of Directors.

Article 8 Effectiveness and Amendment

The Policy shall become effective as of the date of approval by the Board of Directors and the same will be applied for its amendment.