PCSC Personal Information File Security and Maintenance Plan

Chapter 1 Management Responsibilities

Article 1. Purposes

This PCSC Personal Information File Security and Maintenance Plan (hereinafter referred to as the ”Plan”) is established by President Chain Store Corporation (hereinafter referred to as "PCSC") to set forth appropriate measures for the protection of personal data collected, processed, used, and internationally transferred by PCSC (hereinafter referred to as "Personal Information"), with the purpose of enhancing and maintaining its personal data management practice.

Article 2. Scope of application

For the purposes of the Plan, Personal Information refers to the personal data subject to protection under PCSC's Personal Information Protection Management System, includes all personal data collected, processed, used, and internationally transferred by PCSC. Such personal data refers to a natural person's name, date of birth, national identification card number, passport number, physical characteristics, fingerprints, marital status, family information, education background, occupation, medical records, healthcare data, genetic data, sex life, records of physical examination, criminal records, contact information, financial conditions, social activities and any other information that may be used to directly or indirectly identify a natural person.

The Plan applies to all members of PCSC, including but not limited to directors, supervisors, regular and non-regular employees, dispatched personnel and both part-time and full-time staff (“PCSC Personnel”), and is applicable across all organizational units within PCSC.

Chapter 2 Personal Information Protection Management System and the corresponding Policy

To protect the Personal Information it holds, PCSC has established its Personal Information Protection Management System and the corresponding Policy in accordance with the relevant personal data protection laws and regulations of the Republic of China (Taiwan)—including the Personal Data Protection Act and the Regulations Governing the Security and Maintenance of Personal Data Files for the Retail Industry—as well as the Taiwan Personal Information Protection and Administration System (TPIPAS), 2021 edition.

Article 1. Establishment and operation of Personal Information Protection Management System

To operate the Personal Information Protection Management System with efficiency, PCSC has established relevant documentation and assists each department in its effective operation according to the following work schedule. An annual project plan for the upcoming year will be formulated in the fourth quarter of each year, and the work schedule may be adjusted based on actual operational circumstances.

Article 2. Personal Information Protection Management Policy

PCSC proactively creates and delivers services that go beyond customer satisfaction and fulfilling social responsibilities. PCSC further commits to promoting the following measures to ensure the proper use of Personal Information and to prevent any infringement of personal rights for customers, employees, and business partners.

1. Legal compliance

   PCSC strictly complies with the relevant regulations of the Republic of China (Taiwan) regarding the protection of personal data security.

2. Personal Information Management System

   In accordance with the relevant personal data protection laws and regulations of the Republic of China (Taiwan), PCSC has identified internal and external issues that may affect the effectiveness of the Personal Information Management System, as well as the requirements of relevant stakeholders. PCSC has established and announced the Personal Information Management System to PCSC Personnel to clearly define the policies and operational guidelines for Personal Information protection. A cross-departmental Personal Information Management Team has been formed, and appropriate personnel have been assigned to conduct regular inspections, internal audits, and reviews to ensure the effective implementation and continual improvement of the Personal Information Management System. This is to ensure the protection and proper management of Personal Information.

3. Collection, processing and use of Personal Information

   PCSC will collect, process, and use Personal Information within the specific purposes in accordance with the relevant personal data protection laws and regulations of the Republic of China (Taiwan). Appropriate measures will be taken to ensure that the processing and use of Personal Information do not exceed the necessary scope required to achieve the purposes for which the data was provided by the personal data subject.

4. Restrictions on disclosure to third parties

   PCSC will not unlawfully or arbitrarily provide or disclose Personal Information to any third party.

5. Maintaining the accuracy of the Personal Information and safeguarding the exercise of the rights of data subjects.

   To maintain the accuracy of Personal Information and to safeguard the exercise of data subjects' rights, PCSC has established a regular inventory mechanism for Personal Information and related records. PCSC has also formulated rules and procedures to handle data subjects' requests to access, review, supplement, correct, obtain copies of, suspend the collection, processing, or use of, and delete their Personal Information, in order to ensure a prompt and effective response to such requests.

6. Appropriate security and management measures

   PCSC will implement appropriate countermeasures and security management measures based on risk assessments of Personal Information held by each department, in order to prevent unauthorized access, leakage, destruction, or damage of Personal Information.

   When collecting, processing, or using Personal Information through computers or automated machinery, it is required to establish regulations for the use of portable devices or storage media.

   If encryption is required for the retained Personal Information, appropriate encryption mechanisms shall be implemented during its collection, processing, or use.

   When it is necessary to back up Personal Information during operations, appropriate protection shall be applied to the backup data.

   When using network drives or cloud storage, Personal Information protection must be observed, and uploading data arbitrarily is prohibited. Any violations will be handled in accordance with PCSC's disciplinary regulations.

7. Emergency incident response measures

   PCSC's response measures for improper access, loss, destruction, alteration and leakage of Personal Information are as follows: upon confirming a personal data breach, PCSC will promptly take appropriate actions, notify the affected data subjects of the incident, and provide relevant inquiry and resolution channels to prevent significant harm and impact to those data subjects.

8. Training and education

   PCSC provides necessary training to its employees to ensure they understand PCSC's Personal Information Protection Management Policy and related measures.

9. Supervision of commissioned vendors

   When vendors are commissioned to collect, process, or use Personal

Information, PCSC will fulfill its legal obligation to supervise the said commissioned vendors.

10. Policy publication and maintenance

PCSC will announce the Personal Information Protection Management Policy through appropriate means and regularly review the policy to make necessary improvements.

Chapter 3. Establishment of Personal Information Protection Management System

To protect the Personal Information it holds, PCSC has established its Personal Information Protection Management System in accordance with the relevant personal data protection laws and regulations of the Republic of China (Taiwan)—including the Personal Data Protection Act, the Regulations Governing the Security and Maintenance of Personal Data Files for the Retail Industry, the Taiwan Personal Information Protection and Administration System (TPIPAS), 2021 edition, as well as the PCSC's own Personal Information Protection Management Policy.

Article 1. Legal and regulatory review

PCSC shall, in accordance with applicable laws, conduct regulatory identification and compliance procedures related to the Personal Data Protection Act and other relevant regulations, and shall ensure compliance therewith. The process shall include the following:

I. Investigation and acquisition of applicable laws and regulations, including identification and reporting of findings.

II. Review and revision of applicable laws and regulations.

Article 2. Personal Information inventory procedure

To check and identify the Personal Information files held by PCSC, as well as to understand the current status of the collection, processing, and use of such data, PCSC regularly conducts an inventory of Personal Information files and related operational procedures. The results of the inventory are compiled into a “Personal Information Inventory Register.”

I. Personal Information inventory operations

II. Establishment of the Personal Information Inventory Register

III. Review and revision of the Personal Information Inventory Register

Article 3. Risk control procedure

The Personal Information identified through the inventory process is assessed with consideration of both internal and external issues, as well as the needs and

expectations of stakeholders. Based on this, PCSC establishes principles and a framework for risk control, identifies risks and corresponding control measures, conducts risk analysis, and implements necessary countermeasures.

I. Personal Information risk analysis procedure

II. Review of countermeasure plans

III. Review and revision of the risk analysis register

Article 4. Emergency response to the incident

In the event that Personal Information held by PCSC is stolen, leaked, altered, otherwise compromised, or if there is any violation of personal data protection laws or the " Taiwan Personal Information Protection and Administration System" (2021 edition), PCSC shall conduct an investigation and take corresponding actions in accordance with the following procedures:

I. Personal data breach emergency response organization, functional responsibilities, and operating principles

1. In the event of an incident, PCSC Personnel shall promptly report it to the data subject rights protection team and handle the personal data emergency incident in accordance with the PCSC's crisis management procedures.
2. In the event of an incident, the crisis management department shall serve as the emergency response unit, responsible for incident analysis, cross-departmental coordination, notifying the data subjects of the incident, providing channels for follow-up inquiries and resolution, and informing the data subjects of the findings once the investigation is complete.
3. The data subject rights protection team, or the designated crisis management department, shall complete the "personal data breach incident notification and record form" within 72 hours from the time the incident is discovered (or within the timeframe specified by other competent authorities, if applicable), and submit it via email to the relevant government authority. Updates on the handling of the incident shall be provided to the authority as appropriate, depending on the development of the case.
4. The information security operations team is responsible for reporting the incident to the TPIPAS certification authority.
5. The education and training team may include the handling of the incident in the training materials for Personal Information management personnel, to serve as a case study for internal review and learning.
6. The internal evaluation team may incorporate the cause of the incident into audit scopes to prevent similar incidents from occurring again.

II. Incident prevention

1. The data subject rights protection team shall, in accordance with the law and the Plan, prevent the Personal Information held by PCSC from being stolen, altered, damaged, lost, or leaked. It shall also strengthen the control of Personal Information transmission by PCSC Personnel, both internally and externally, to prevent data breaches.
2. The information security operations team and the internal evaluation team shall jointly supervise all departments to monitor the usage of Personal Information within each department in accordance with various standard operating procedures.
3. The education and training team is responsible for enhancing PCSC Personnel's education and awareness to reduce the frequency of personal data incidents.

III. Incident handling

1. When PCSC Personnel discovers any abnormal signs that may be related to a potential personal data breach, the discoverer shall immediately notify the data subject rights protection team. The crisis management department shall investigate the cause of the abnormality and assess whether it constitutes a personal data incident.
2. If it is determined not to be a personal data incident, the data subject rights protection team shall arrange for the responsible units to continue monitoring the situation until the abnormality is resolved or eliminated. If it is determined to be a personal data incident, the following assessments shall be conducted:
   (1) Scope of impact, including affected systems, applications, or Personal Information files.
   (2) Source and cause of the incident.
   (3) Extent of the loss.
   (4) Possible responsive measures.
   (5) Required support for response actions.

IV. Preventing recurrence of similar incidents

The data subject rights protection team is responsible for documenting and archiving the analysis of the incident's cause, improvement measures, specific actions to prevent similar incidents, as well as audit trails and related evidence collected during the response and recovery process. This information shall assist the education and training team in developing internal case studies for review and learning.

Chapter 4. Implementation of Personal Information Protection

Management System

To protect the Personal Information it holds, PCSC has established its Personal Information Protection Management System in accordance with the relevant personal data protection laws and regulations of the Republic of China (Taiwan)—including the Personal Data Protection Act, the Regulations Governing the Security and Maintenance of Personal Data Files for the Retail Industry, the Taiwan Personal Information Protection and Administration System (TPIPAS), 2021 edition, as well as the PCSC's own Personal Information Protection Management Policy- and has implemented it in accordance with the provisions set forth in this Chapter 4.

Article 1. Development of implementation procedures

To operate the Personal Information Protection Management System with efficiency, PCSC has clearly defined the implementation procedures in the Plan and related internal rules, and will announce them to PCSC Personnel to ensure full awareness.

Article 2.Basic principles for the collection, processing, use, and international transfer of Personal Information

PCSC will collect, process, use, and internationally transfer Personal Information in an honest and good-faith manner, without exceeding the necessary scope of specific purposes, and with legitimate and reasonable relevance to the purposes of collection, while complying with the following requirements:

I. Collection of Personal Information

If the collected Personal Information is not provided by the data subject, the data subject shall be informed of the source of their personal data and the matters required to be notified as stated in the preceding paragraph, prior to any processing or use. If the data subject expresses refusal to provide their personal data, PCSC shall cease to process and use such data.

II. Processing of Personal Information

For establishment or use of Personal Information files, activities such as the recording, input, storage, editing, correction, duplication, retrieval, deletion, output, linkage, and internal transmission of Personal Information shall comply with applicable personal data protection laws and regulations. The scope and authority of personnel in each department who may access the Personal Information, as well as those designated to handle Personal Information, shall be clearly defined.

III. Use of Personal Information

If PCSC intends to use the Personal Information it holds for purposes other than the specified purpose, it shall first review whether such use complies with the

provision of Paragraph 1, Article 20 of the Personal Data Protection Act.

IV. Use of Personal Information for commercial marketing

1. When PCSC uses Personal Information for commercial marketing purposes, it shall, in accordance with the Personal Data Protection Act, provide the data subject with a free method to refuse such marketing at the time of the first communication.
2. If the data subject did not express a refusal at the time of the initial marketing, the data subject may still refuse through the channels and methods provided by PCSC. Upon receiving the data subject's refusal, PCSC shall immediately cease the use of their personal data.

V. Restrictions on the collection, processing, and use of sensitive personal data

PCSC shall not collect sensitive personal data relating to medical records, healthcare, genetics, sex life, physical examination and criminal records, except as otherwise provided in the provision of Article 6 of the Personal Data Protection Act.

VI. International transfer of Personal Information

When transmitting Personal Information, necessary protective measures should be taken to prevent leakage. Before transferring data subject's Personal Information internationally, it is necessary to verify whether there are any restrictions imposed by the central competent authority and to inform the data subject of the intended destination country or region.

Article 3. The rights of data subjects.

The data subject, in accordance with the Personal Data Protection Act, has the right to inquire about and review their personal data, request a copy of such data, request supplementation or correction, demand the cessation of the collection, processing, or use of such data, and request its deletion. The data subject may also submit complaints or inquiries related to the aforementioned matters to PCSC. PCSC shall respond honestly and promptly, and handle such requests and maintain related records in accordance with the "Procedures for Exercising the Rights and Handling Complaints of Personal Data Subjects" and the "Regulations on the Management of Personal Information Documents and Records."

Article 4. Management and supervision

PCSC shall manage and supervise the Personal Information it holds with regard to the following matters:

I. Maintaining the accuracy of Personal Information

II. Security management measures and management of PCSC Personnel.

III. Supervision of entrusted processing of Personal Information

Article 5. Training and education

I. Principles

To operate the Personal Information Protection Management System with efficiency and to enable PCSC Personnel to have the correct understanding and capability in managing Personal Information, PCSC shall provide necessary management education and training to PCSC Personnel.

II. Training and education for Personal Information protection and management

1. PCSC Personnel shall receive at least one basic training on the Personal Data Protection Act or related management regulations during their term of employment.
2. In addition to the aforementioned training, members of Personal Information Management Team may also participate in advanced courses related to information security, privacy protection, and security measures, and shall promote the learned content to their respective units after the training.

III. Measures to maintain and improve performance

1. After the training course, an appropriate assessment shall be conducted through testing. If the test results do not meet the required standard, supplementary training will be provided.
2. The education and training team shall compile the results of the training assessments and report the effectiveness of the training to the personal data management representative of PCSC.
3. In the event of any violation of personal data protection regulations, the supervisor of the relevant department shall be notified. The incident will be recorded and included in the individual's performance evaluation. In cases of serious violations, disciplinary action will be taken in accordance with PCSC's internal regulations on rewards and penalties.

Article 6. Dispose of personal data upon business termination

Upon termination of business operations, PCSC shall destroy or delete related Personal Information, except for data required to be retained by competent authorities or applicable laws. Personal Information shall be disposed of within the retention period specified in the Personal Information Inventory Register maintained by each business unit. For physical (paper-based) Personal Information, disposal shall be carried out through shredding, outsourced incineration, or water-based destruction. For Personal Information stored on servers, disk arrays, magnetic tapes, or portable storage media, Personal Information shall, in principle, be deleted through formatting.

If the device or storage media is no longer in use and is being decommissioned, measures such as degaussing, cutting, or striking shall be adopted to prevent Personal Information leakage from such media.

Chapter 5. Control and improvement of Personal Information Protection Management System

Article 1. Responsibility of management

To ensure effective control of the Personal Data Protection Management System, PCSC shall appoint appropriate personnel with the following responsibilities and duties:

I. Top Management

The top executive of PCSC, who is responsible for overall business management, shall have the following responsibilities:

1. Determining the purporses of the Personal Data Management System to ensure alignment with PCSC's needs and development strategy.
2. Establishing the Personal Data Protection Management Policy.
3. Making decisions regarding resource management.
4. Defining the organizational structure and division of responsibilities for personal data protection management.
5. Periodically reviewing the management system to ensure it attains the intended objectives.
6. Establish an effective communication mechanism to provide timely guidance and support to PCSC Personnel.
7. Communicating the importance of implementing the Personal Data Management System.

II. The personal data management representative

The top executive of PCSC shall appoint one of the management members as the personal data management representative. The responsibilities and authorities of this representative shall include:

1. Being responsible for maintaining the effectiveness of the Personal Information Protection Management System and establishing the necessary internal personnel structure.
2. Ensuring fairness and objectivity in the execution of duties.
3. Ensuring that all processes required by the Personal Information Protection Management System are established, implemented, and maintained.
4. Reporting to top executive of PCSC on the performance and improvement measures of the Personal Information Protection Management System.

III. Personal data management personnel

Personal data management personnel refers to individuals who assist in and

continuously support the operation of PCSC's Personal Information Protection Management System. These personnel may include Certified Project Management Professional (CPMP), Certified Personal Information Assurance Professional (CPIA), or Certified Personal Information Auditor (CPA), as well as those assigned by each department who have completed relevant personal data protection training. They are responsible for executing personal data management projects within their respective departments and for actively promoting and ensuring the effective operation of the Personal Information Protection Management System.

IV. Internal personal data assurance

Internal assurances are personnel who have obtained internal personal data management qualifications within PCSC or are Certified Personal Information Assurance Professional (CPIA). They are responsible for conducting internal audits to assess the effectiveness of PCSC's implementation of the Personal Information Protection Management System.

Article 2. Effectiveness measurement

To ensure the continuous and effective operation of the Personal Data Management System, PCSC shall regularly conduct analysis and measurement according to the following procedures and maintain related records:

I. Establish measurement items.

II. Implement measurements.

III. Evaluate the effectiveness of measurement results.

IV. Preserve measurement data.

Article 3. Document control

PCSC shall manage the preparation and retention of key documents that constitute the Personal Information Protection Management System in accordance with the "Regulations on the Management of Personal Information Documents and Records" These documents include:

1. Personal Information Protection Management Policy.
2. The Plan (personal data protection management manual), along with related internal management rules and procedures.
3. Other records required for the implementation of the Personal Information Protection Management System.

Article 4. Internal control

To verify and ensure that the operation of the Personal Information Protection Management System complies with legal requirements, as well as the Personal

Information Protection Management Policy and the requirements of the Plan, PCSC shall establish an internal control management system. Internal audits shall be conducted annually on a regular basis through the following procedures:

I. Preparation for internal audit

II. Execution of internal audit procedures

III. The personal data management representative, audit personnel, or responsible department supervisors shall continuously follow up on the status of improvements to prevent recurrence of issues.

Article 5. Improvement

I. Regular review

To implement effective personal data protection management, the personal data management representative shall convene regular annual meetings with relevant responsible personnel to review the Personal Information Protection Management System. The results of the review shall be recorded and reported to the top executive of PCSC.

II. Continuous improvement

When the top executive of PCSC makes decisions to adjust the Personal Information Protection Management System, the following factors shall be considered to guide the adjustments and revisions:

(1) Review reports.

(2) Changes in societal conditions, public awareness, and technological developments.

(3) Changes in the company's business scope.

(4) Internal and external suggestions for improvement.

(5) Any other changes that may affect the Personal Information Protection Management System.

III. Corrective and preventive measures

PCSC shall plan and implement corrective and preventive measures based on the procedures established for handling nonconformities and potential risks identified through internal control results. The following actions shall be taken during the execution of these measures:

1. Corrective Measures

(1) Identify the details of the nonconformity and determine its root cause.

(2) Assess needs and propose a corrective plan to prevent recurrence.

(3) Set a reasonable execution timeline.

(4) Record the results of implementation.

(5) Review the effectiveness of the corrective plan.

2. Preventive measures

(1) Identify the content and causes of potential nonconformities based on the risks associated with holding Personal Information.

(2) Assess whether the risks posed by potential nonconformities are acceptable; if not, propose a preventive improvement plan.

(3) Set a reasonable execution timeline.

(4) Record the results of implementation.

(5) Review the effectiveness of the corrective plan.

(6) Continuously improve the Personal Information Protection Management System.