## 一、目的

為規範個人資料(以下簡稱「個資」)之蒐集、處理及利用，避免人格權受侵害，並促進個人資料之合理利用，參照<個人資料保護法>(以下簡稱「個資法」)精神，訂定此辦法。

## 二、範圍

凡屬自然人，包括應徵者、在職員工、離職員工、客戶代表及廠商代表等皆適用(以下簡稱「當事人」)。

## 三.、定義

(一)個人資料

姓名、出生年月日、身分證字號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務狀況、社會活動及其他得以直接或間接方式識別該個人之資料。(其中醫療、基因、性生活、健康檢查、犯罪前科屬特種個人資料，原則上不得蒐集、處理或利用，但法律明文規定者除外。)

(二)個人資料形式

凡以紙本、檔案、系統等留存的個人資料皆在此辦法規範內。

(三)蒐集

指以任何方式取得個人資料，並應進行告知。

蒐集的要件應有特定目的及特定情形(例：法律明文規定、與當事人有契約或類似契約關係、經當事人書面同意等...)。

(四)處理

包括紀錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。

處理的要件應有特定目的及特定情形(例：法律明文規定、與當事人有契約或類似契約關係、經當事人書面同意等...)。

(五)利用

將蒐集之個人資料為處理以外之使用。

利用的要件應於蒐集的特定目的內為之。

(六)告知

蒐集個人資料時應明確告知當事人下列事項：

1. 公司名稱。
2. 蒐集之目的。
3. 個人資料之類別。
4. 個人資料利用的期間、地區、對象及方式。
5. 當事人權利。
6. 當事人得自由選擇提供個人資料時，不提供將對其權益之影響。

7. 蒐集非由當事人提供之個人資料，應於處理或利用前，告知個資當事人資料取得來源及第 1 至第 5 項所列事項。

(七)個資保管人

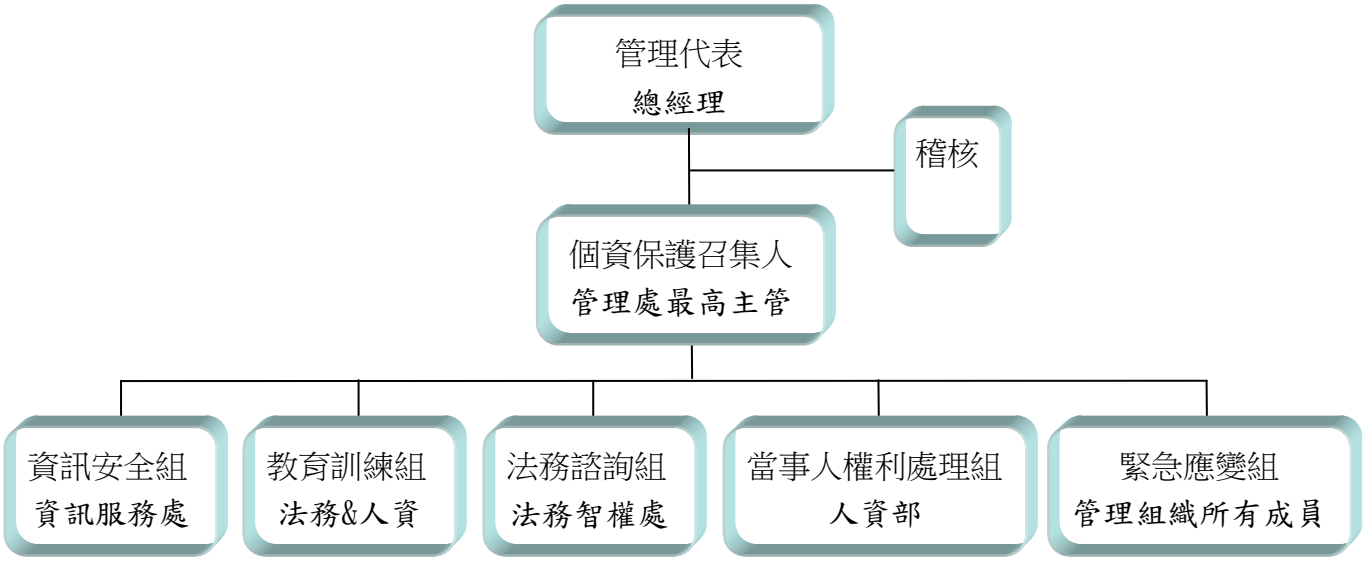
指保有個人資料之人員或單位(應徵者或在、離職員工之個資一律保管在人資單位)。

(八)個資法規範對象

自然人、法人或其他團體(所以每個人都必須遵循個資法)。

## 四、管理規定

(一)個資保護管理組織




(二)組織各層級職責

個資保護管理組織最主要任務在於極力保護個人資料安全，維護當事人權益，預防個資被竊取、被竄改、毀損、滅失或洩漏，並將個資保護意識宣達給全公司員工。

1. 管理代表：

全公司個資保護管理代表。

2. 個資保護召集人：

由管理處最高主管擔任，統籌全公司個人資料保護相關規定及做法，定期檢視個資管理措施之有效性。

3. 稽核：

由集團營運處擔任，負責訂定稽核制度且定期稽核公司個資安全保護措施，並提出缺失，督導改正。

4. 資訊安全組：

由資訊服務處擔任，負責訂定資訊安全維護相關辦法，維護公司載有個人資料之系統安全，採取必要措施有效預防個資被竊取、被竄改、毀損、滅失或洩漏，並留下使用紀錄、軌跡資料及證據保存。

5. 教育訓練組：

由人資部與法務智權處共同負責，執行全公司個資安全維護認知宣導與教育訓練。

6. 法務諮詢組：

由法務智權處負責，提供個資相關法律諮詢，協助釐清個資法問題。

7. 當事人權利處理組：

由人資部擔任窗口，負責管理全公司(含在離職)員工個人資料，當事人遇有個資疑義、申訴及權利請求時之接洽單位。

8. 緊急應變組：

個資保護管理組織中所有成員共同參與，並依事故預防通報應變程序處理，若發生緊急重大事件，例如個資檔案毀損、滅失、被竊取或有違反個資保護之行為造成公司損害時，公司發言人應共同參與。

(三)當事人權利

1. 除以下第(4)及第(5)點，因執行職務或業務或依法律另有規定外，當事人就其個人資料得行使以下權利。

(1)查詢或請求閱覽。

(2)請求製給複製本。

(3)請求補充或更正。

(4)請求停止蒐集、處理或利用。

(5)請求刪除。

2. 當事人提出前款權利請求時，在職員工得經由內部資訊系統提出，非在職員工需填寫<個人資料申請書>提出申請。在職員工之承辦人為人資部，非在職員工之承辦人為當事人權利處理組。

3. 當事人提出第(1)點或第(2)點請求時，承辦人應於 15 天內提供，若延期或不提供應在期限內書面回覆當事人原因。

4. 當事人提出第(3)點、第(4)點或第(5)點請求時(在職員工僅得提出第(3)點請求)，承辦人應於 30 天內處理之，若延期或不核准申請應在期限內書面回覆當事人原因。個資保管人負有主動或依當事人要求維護個人資料正確之義務。

5. 當事人為應徵者或在離職員工，其權利已詳述於人事管理相關表單中。

6. 第 5 點外之當事人，其個人資料之蒐集、處理、利用，應在特定目的範圍內且須告知當事人應告知事項及權利，並應提供當事人拒絕接受行銷之方式。

(四)除外規定

以下各項為依相關法律規定及管理需求，得不經告知，蒐集、處理、利用個人資料。

1. 在職員工：依勞動基準法第 7 條規定應置備勞工相關資料，故在職員工需提供其個人資料，並不得要求刪除。
2. 離職員工：依勞動基準法第 7 條規定，勞工資料應保管至勞工離職後五年，員工離職五年後可填寫<個人資料申請書>向當事人權利處理組提出申請刪除其個資。
3. 健康檢查：依職業安全衛生法第 12 條及勞工健康保護規則第 11 條與第 12 條規定，雇主對在職勞工應施行定期健康檢查，檢查紀錄至少應保存七年，勞工對於健康檢查有接受之義務。相關健康檢查紀錄皆保管在人資部，且謹遵勞工健康保護規則第 16 條，對於勞工體格及健康檢查紀錄之處理，應保障勞工隱私權。
4. 醫療資料：依勞工請假規則第 10 條規定，辦理請假手續時，雇主得要求勞工提出有關證明文件。

(五)個資保護宣告

1. 有契約關係者(例：員工)，因人事管理需求得蒐集、處理、利用個人資料;其餘因經營管理需求對於個資之蒐集、處理、利用均依規定告知當事人並取得當事人同意。
2. 對於蒐集之個人資料僅處理、利用在特定目的上，並依相關法規或在特定目的消失時停止處理、利用個人資料。
3. 公司嚴密保護當事人的個人資料，未經當事人同意，絕不會交予、透露及販賣給第三者或其他非關係企業，並妥善存放於公司資料庫中。
4. 有接觸個人資料之員工皆嚴格遵守上述個人資料蒐集、處理、利用原則並負有保密責任，絕不外洩或利用於其他用途上，且不允許未獲授權者使用，不使當事人因個資外洩而受不利影響，遇有個資問題則參照個人資料保護法或本管理辦法或洽詢法務諮詢組。

## 五、風險管控措施與事故預防通報應變程序

(一)日常管理處理程序

1. 個人資料經過盤點，有效控管讀取人員權限，非個資保管人不保有個資，每位員工皆應檢視並將手邊個資交回個資保管人。
2. 載有個人資料之文件在特定目的消失，停止處理、利用後，應完全銷毀，嚴禁做為回收紙再利用。
3. 個資保管人應謹慎保管個人資料，不可將載有個資之文件或檔案隨意放置或開啟，使他人容易取得或讀取。
4. 制定<個人資料運用、保護與保密條款>置於<聘僱合約書>中，凡新進員工皆於正式報到一週內簽署該合約書，並透過公司內部資訊系統將<聘僱合約書>改版公告給每

位在職員工。

5. 致力將個資保護觀念灌輸給每位員工，在職人員由教育訓練組進行個資保護宣導並將個人資料保護相關法規及此辦法公告於公司內部資訊系統，新進人員由人資單位於新人訓練課程中宣導。
6. 資訊安全組制定資訊安全維護相關辦法及採取必要措施，設置防火牆防止外部駭客入侵，裝設掃毒軟體，定期掃毒，以提供更安全的系統環境。內部個人資料系統皆留下使用紀錄、軌跡資料及證據保存，資料庫並定期做適當備份，且至少保存五年。
7. 提供當事人諮詢、處理、提出建議與權利請求的管道，並將過程與結果做成紀錄以作為日後改善的參考。
8. 遇個資爭議事件應由法務諮詢組與當事人權利處理組研討應變措施，並妥善保存所有與公司外部專家、政府機關、新聞媒體、個資當事人等往來文書，嚴禁任意變更或刪除銷毀，以利後續稽核並避免不必要糾紛，且至少保存五年。

(二)重大個資事故處理程序

判定為重大個資事故時，例：公司網站遭駭客入侵，致大量會員或員工等之個資外洩;或個資檔案毀損、滅失或被竊取等...。個資保護管理組織應立即會同公司發言人召開緊急會議向公司負責人報告，並採取補救措施，且應以適當方式通知當事人，如有需要應向外部專家(如：律師或顧問)尋求協助，並向警政或檢調單位報案及召開記者會發布聲明稿。並檢討訂定預防再次發生之措施。

## 六、懲處規定

員工與公司皆屬個資法規範對象，觸犯個資法須負民事、刑事或行政責任，故每位員工都應謹慎以對，違反個資法或本管理辦法者，經查證屬實，除依法處置外並將進行內部懲處。

(一)依法處置

依個資法及相關法律之罰責處理。

(二)內部懲處

1. 小過：因疏忽使個人資料暴露在公開場合或被他人知悉，但情節較輕且未造成當事人或公司損害者。
2. 大過：違反個資法或本管理辦法有關蒐集、處理、利用個資之規定，或拒絕當事人行使其權利，受當事人申訴致公司名譽受損。
3. 免職：故意洩漏或利用個人資料謀取非法利益，或擅自變更個人資料，足生損害於他人，或違反個資法或本管理辦法有關蒐集、處理、利用個資之規定，致公司或公司負責人發生損害賠償或被主管機關處罰者。

## 七、實施與修改

本辦法經個資保護管理組織之管理代表核准後公佈實施，修改時亦同。

## 八、附件

(一)個人資料申請書

Article 1 **Purpose**

These guidelines are formulated in accordance with the Personal Information Protection Act （hereinafter "the Act") to govern the collection, processing and use of personal information so as to prevent harm on personality rights, and to facilitate the proper use of personal information.

Article 2 **Scope**

All natural persons, including the applicant, in-service employees, former employees, customer representatives and vendor representatives are applicable (hereinafter "the party") .

Article 3 **Definition**

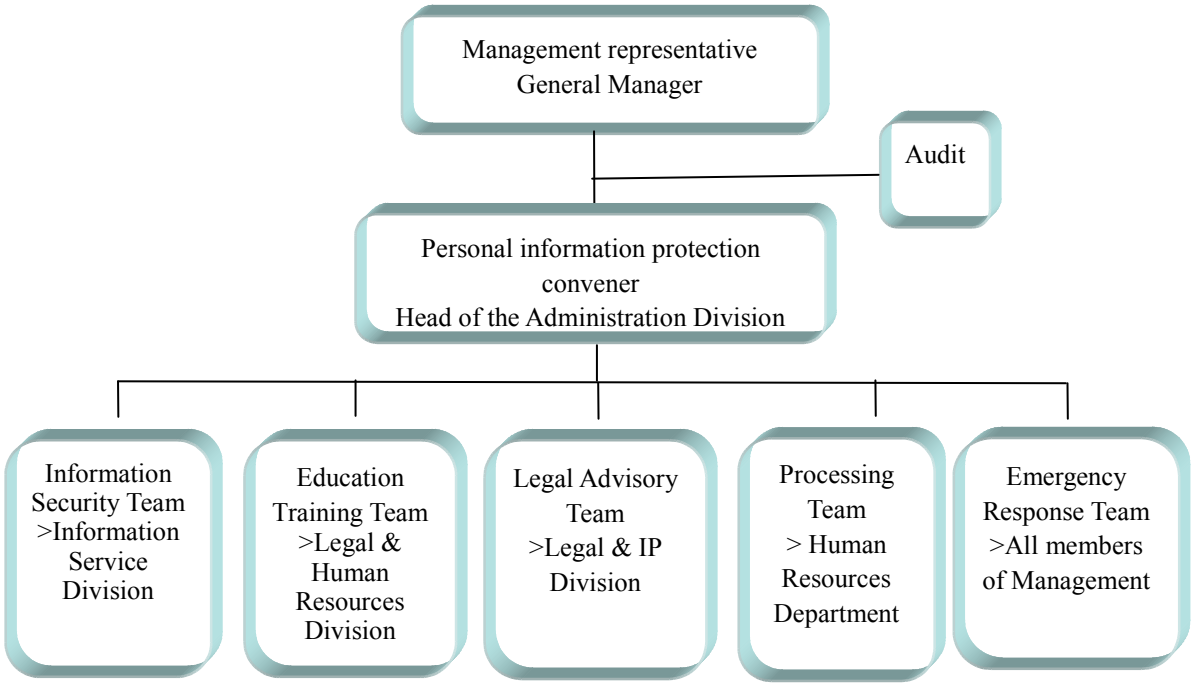
1. Personal information
   Name, date of birth, I.D. Card number, passport number, characteristics, fingerprints, marital status, family, education, occupation, medical record, medical treatment, genetic information, sexual life, health examination, criminal record, contact information, financial conditions, social activities and other information which may be used to identify a natural person, both directly and indirectly. (Personal information of medical treatment, genetic information, sexual life, health examination and criminal records should not be collected, processed or used. However, those defined in the regulations are not subject to the limits set in the preceding sentence.)
2. Forms of personal information
   All personal information retained in paper, files, systems are within the norms of these guidelines.
3. Collection
   Collecting personal information in any form and way, and a declaration of intention must be made.
   The collection shall be made with a specific purpose and for a specific condition (such as following laws and regulations, having a contractual relationship with the party, with a written consent of the Party, etc.).
4. Processing
   Includes record, input, store, compile, correct, duplicate, retrieve, delete, output, connect or internally transmit information. The processing shall be made with a specific purpose and for a specific condition (such as following laws and regulations, having a contractual relationship with the party, with a written consent of the Party, etc.).
5. Use
   All methods of personal information use other than processing.
   The personal information shall be used for the specific purpose of collection.
6. Inform
   The following items should be told precisely to the Party when collecting personal information:
   (1) company name
   (2) purpose of collection
   (3) classification of the personal information
   (4) time period, area, target and way of the use of personal information
   (5) rights of the Party
   (6) the influence on his rights and interests while the Party chooses not to provide his personal information
   (7) The Company should notify the Party of the source of information and Item 1 to 5 of Paragraph 1 of the preceding Article, before processing or using personal information which was not provided by the Party.
7. Keeper of personal information
   Refers to the person or unit that keeps personal information (the personal information of

the applicants or the in-service/former employees shall be kept in the Human Resource Department).

8. The subject regulated by the Act
   Natural persons, legal persons or other groups (so everyone must follow the Act).

Article 4 **Management regulations**

1.Personal Information Protection Management Organization




2.Responsibilities of all levels of the organization

The main task of the personal information protection management organization is to protect personal information security, protect the rights and interests of the party, prevent theft, tampering, damage, loss or leakage of personal information, and publicize the awareness of personal information protection to employees throughout the Company.

(1) Management representative :
The personal protection management representative of the Company

(2) Personal information protection convener :
Undertaken by the head of the Administration Division, coordinating the Company's personal information protection regulations and practices, and regularly reviewing the effectiveness of the personal information measures.

(3) Audit :
Undertaken by the Operation Division, responsible for setting auditing policies and regularly auditing the personal information measures, and finding defects for correction.

(4) Information Security team:
Undertaken by the IT Services Division, responsible for setting IT security maintenance measures to protect the Company’s systems containing personal information, to take the necessary measures to effectively prevent personal information from being stolen, altered, destroyed or disclosed, and to keep records, traces and evidences.

(5) Education and Training Team:
Undertaken by the Human Resources Department and the Legal & IP Division, responsible for the implementation of company-wide personal information training.

(6) Legal Advisory Team:

Undertaken by the Legal & IP Division, responsible for providing relevant legal advice to help clarify the regulations of personal information.

(7) Processing Team:
Undertaken by the Human Resources Department, responsible for managing the personal information of all employees (including former employees) of the Company, and acting as the connect window for handling doubts, appeals and claims requested by the party.

(8) Emergency Response Team:
Undertaken by all members of personal information protection management organization. This team shall follow the incident response procedures to handle related matters. If a major emergency occurs, for example, personal information are damaged, destroyed or stolen, or violations of the Act causing damage of the Company, the spokesman of the Company should jointly participate.

3. The rights of the party

(1) The party may exercise the following rights with respect to their personal information. Performing item (d) and item (e) listed below may need to refer to the regulations set in other statutes due to the party's duties or business.
   (a) Query or request to read
   (b) Request for a copy
   (c) Request for supplementation or correction
   (d) Request to stop collecting, processing or using
   (e) Request to delete

(2) When the party requests for matters listed in the preceding paragraph, the information could be obtained from the internal information system for the in-service employee, and the former employee must fill out the "Personal Information Application Form" to apply. The human resources department is responsible for handling matters for the in-service employees; the processing team is responsible for handling matters for the former employees.

(3) When the request listed in (a) or (b) is made by the party, the responsible person shall provide it within 15 days. If it could be delayed or not to provide, a reason shall be provided in writing within the time limit.

(4) When the request listed in (c), (d) or (e) is made by the party (the in-service employee can only request for (c)), the responsible person shall provide it within 30 days. If it could be delayed or not to provide, a reason shall be provided in writing within the time limit. The keeper of personal information has the obligation to take the initiative or to maintain the correctness of personal information as required by the party.

(5) The rights of the applicants or the former employees are detailed in the HR-related forms.

(6) The collection, processing and use of the personal information of the party, except those persons mentioned in (5), shall be within a certain range of purpose, and the Company shall notify the party the related issues and rights, and the measures of refusal at the first marketing action.

4. Exclusion regulations

The following items are collected, processed, and used without prior notice in accordance with relevant legal requirements and management requirements.

(1) In-service employees: According to Article 7 of the Labor Standards Act, labor-related information shall be retained. Therefore, the in-service employees are required to provide their personal information and may not request deletion.

(2) Former employees: According to Article 7 of the Labor Standards Act, labor information shall be kept for five years after the employee leaves the company. After five years of resignation, the employee can fill out the "Personal Information Application Form" to request the Processing Team to delete his/her personal information.

(3) Health check: According to Article 12 of the Occupational Safety and Health Act and Articles 11 and 12 of the Labor Health Protection Rules, employers shall take regular health checks conducted by the Company. The inspection records shall be kept for at least 7 years. Relevant health check records shall be kept in the Human Resources Department. Employees' privacy shall be protected when handling the health check records of the employees in accordance with Article 16 of the Labor Health Protection Rules.

(4) Medical information: According to Article 10 of the Regulations of Leave-Taking of Workers, when applying for leave, the employer may ask the worker to submit relevant supporting documents.

5. Declaration of personal information protection

(1) The Company may collect, process, and use personal information of those who have contractual relationships (e.g. employees) with the Company for personnel management needs; the collection, processing, and use of personal information of other individual for business management needs shall be informed to the party and obtain the party's consent.

(2) The collection of personal information shall only be processed and used for specific purposes. Processing and using personal information shall be stopped according to relevant regulations or when the specific purpose disappears.

(3) The Company shall strictly protect the personal information of the party and will never hand over, disclose and sell them to third parties or other non-relational enterprises without the consent of the party, and will be properly stored in the Company's database.

(4) Employees who have rights to access to personal information shall strictly abide by the above principles of collection, processing and use of personal information and are responsible for confidentiality. They shall not disclose or use it for other purposes, prohibit unauthorized persons to use it, and prevent the party from being harmed due to personal information disclosure. In case of personal information issue, refer to the Personal Information Protection Act or these Guidelines or consult the Legal Advisory Team.

Article 5 **Risk management measures and incident prevention notification response procedures**

1. Daily management procedures

(1) After the personal information is checked, the access permission shall be effectively controlled. The personal information shall not be kept by a person who is not responsible for keeping personal information. Each employee shall hand over the personal information to the keeper of personal information.

(2) The document containing personal information disappears shall be completely destroyed when the specific purpose no longer exist, and when processing and use are stopped. It is strictly forbidden to reuse it as recycled paper.

(3) The keeper shall keep the personal information cautiously. Do not arbitrarily place or open the documents or files containing personal information for others to easily obtain or read them.

(4) Formulate "Rules for using, protecting and securing personal information" in "Employment Contract". All new employees are to formally signed back the contract within a week after onboard. The Company shall revise the "Employment Contract" through internal information system and announce it to each employee.

(5) Committed to instilling the concept of personal information protection into each employee. The Education Training Team shall promote the personal information protection concept, and publish regulations related to personal information protection and these Guidelines in the Company's internal information system. The new employees shall be educated by the HR department in the newcomer training.

(6) The Information Security Team shall formulate guidelines and related measures to take for information security maintenance, set up a firewall to prevent external

hackers from invading, install anti-virus software, and regularly scan for virus to provide a safer system environment. Records, traces and evidences of the internal for storing personal information shall be kept. The database shall be backed up regularly and kept for at least five years.

(7) Provide a channel for the party to consult, process, make recommendations and claim rights, and record the process and results as a reference for future improvement.

(8) In case of a personal information incident, the Legal Advisory Team shall discuss with the Processing Team to provide contingency measures, and properly save all the documents for communicating with external experts, government agencies, media, and the party to facilitate future audits and to avoid unnecessary disputes. It is prohibited to change or delete these documents. These documents shall be saved for at least five years.

2. Procedures for handling major personal information incident

When a major personal information incident occurs, like the Company's website is hacked, causing disclosure of a large amount of personal information of members or employees, or the files containing personal information are damaged, destroyed or stolen, the personal information protection management organization shall immediately host an emergency meeting with the Company's spokesman to report to the person in charge of the Company, and take remedial measures, and shall notify the party in an appropriate manner, if necessary, ask external experts (such as lawyers or consultants) for assistance, call the police or prosecutors to file a report, and hold a press conference to release a statement. Review and formulate measures to prevent recurrence.

Article 6 **Punishment**

The employees and the Company are both the objects regulated in the Act. The person violating the Act must bear civil, criminal or administrative liabilities. Therefore, every employee shall be cautious about it. Anyone who violates the stipulations of the Act or these Guidelines shall be punished internally as well.

1. Disposed according to law

Dispose according to the Act and related laws.

2. Internal punishment

(1) Minor demerit: Inadvertently exposing personal information to public or being known to others, but in less serious circumstances and without causing damage to the party or the Company.

(2) Major demerit: Violation of the Act or these Guidelines on collecting, processing, and using personal information, or refusing the party to exercise their rights so that the reputation of the Company is damaged due to the party's complaints .

(3) Dismissal: deliberately disclosing or using personal information for illegal gains, or arbitrarily changing personal information, causing damage to others, or violating the Act or these Guidelines on collecting, processing, and using personal information, causing damage to the Company or the responsible person or punishment by the competent authority.

Article 7 **Enforcement and revision**

These Guidelines shall be implemented after the management representative of the Personal Information Protection Management Organization grants the approval. The same procedure shall be followed when the guidelines have been amended.

Article 8 **Annex**

1. Personal Information Application Form