

**Fubon Financial Holding Co., Ltd. and
Subsidiaries
Guideline for Security Measures for the
Personal Information File and the Handling for
the Personal Information After Termination of
Business**

Document No. : FHC-O-PDP-3-20241203
Approval Date : December 03, 2024
Effective Date : December 03, 2024
Responsible Unit : Risk Management Division, Operational Risk
& Planning Department
Version : Version 13

Content

| | | |
|-------------------|---|-----------|
| Chapter 1 | General Rules | 3 |
| Chapter 2 | Allocate management personnel and significant resources | 3 |
| Chapter 3 | Define the scope of personal information | 4 |
| Chapter 4 | Personal information Risk Assessment | 6 |
| Chapter 5 | Use Records, Trace Information, and Evidence Preservation | 7 |
| Chapter 6 | Overall Continuous Improvement for Personal Information Security Maintenance | 7 |
| Chapter 7 | Definition and Explanation | 7 |
| Chapter 8 | Personal Information Collection | 8 |
| Chapter 9 | Personal Information Processing and Use | 10 |
| Chapter 10 | Commissioned Collection, Processing, and Use of Personal Information | 13 |
| Chapter 11 | Procedures for claiming and exercising party's rights | 14 |
| Chapter 12 | Acceptance of exercise of the Party's rights | 15 |
| Chapter 13 | Handling and Response to Exercise of the Party's Rights | 16 |
| Chapter 14 | Personnel Management | 17 |
| Chapter 15 | Operation Management | 18 |
| Chapter 16 | Information Equipment Management | 21 |
| Chapter 17 | Physical Environment Security | 23 |

| | | |
|--|--|-----------|
| Chapter 18 | Prevention of personal information incidents | 24 |
| Chapter 19 | Reporting of Personal Information Incidents | 24 |
| Chapter 20 | Responsive Mechanism for General Personal Information Incidents | 25 |
| Chapter 21 | Responsive Mechanism for Important Personal Information Incident specified by the Company or Major Personal Information Incident specified by the FSC (hereinafter referred to as the “important personal information incident and major personal information incident) | 26 |
| Chapter 22 | Personal Information Handling Procedures after the Termination of Business | 27 |
| Chapter 23 | Personal Information Files Management after Termination of Business | 27 |
| Chapter 24 | Personal Information Protection and Management Educational Training | 28 |
| Chapter 25 | Audit and Improvement Procedures | 29 |
| Chapter 26 | Others | 29 |
| Table: Record of Changes | | |
| Attachment 1: Personal Information Infringement Incident Reporting Form | | |
| Attachment 2: Personal Information Infringement Incident Reporting and Recording Form | | |

Chapter 1 General Rules

Article 1. Purpose of Establishment

To guide Fubon Financial Holding Co., Ltd. (“the Company”) and the Company’s subsidiaries listed on its business license (“subsidiaries”) in implementing personal information file security maintenance and management, preventing personal information from being stolen, altered, damaged, destroyed, leaked or abuse of use, and specifying the personal information handling method after the termination of business, and to facilitate compliance, the “Fubon Financial Holding Co., Ltd. and Subsidiaries Guideline for Security Measures for the Personal Information File and the Handling for the Personal Information After the Termination of Business” (“the Guideline”) has been established according to the “Personal Information Protection Policy” of the Company.

Article 2. Applicable Scope

The applicable scope of the Guideline shall include the Company and its subsidiaries. Where the relevant laws of local governments or regions of overseas subsidiaries specify other requirements, such laws and regulations shall prevail.

Except where the competent authority requires that “Guidelines for Security Measures for Personal Information Files and the Handling of Personal Information after the Termination of Business” be separately established, subsidiaries may follow this Guideline or establish their own. If they follow this Guideline as their “Guidelines for Security Measures for Personal Information Files and the Handling of Personal Information after the Termination of Business,” it should be approved at the appropriate level of authority of the subsidiary. Subsidiaries shall also follow the principles of this Guideline in supervising their own subsidiaries.

Chapter 2 Allocate management personnel and significant resources

Article 3. Establishment of a Personal Information Protection and Supervision Committee

The Company establishes the “Personal Information Protection and Supervision Committee” under the Risk Management Executive Committee in order to supervise the relevant personal information protection matters. The personal information protection supervisory unit is handled by the Operational Risk & Planning Department of the Risk Management Division in order to assist with the establishment of a personal information protection system, operation, and relevant educational training.

Article 4. Achieving the Objectives of Personal Information Protection Management

Each unit supervisor shall act as the responsible person for personal information protection management work in each unit. Each unit supervisor shall be responsible for the compliance with the personal information protection management policies and relevant regulations, and shall also assign

personnel to handle personal information protection and management related works, In order to ensure the realization of the company's objectives for personal information protection and management; each unit should comply with the following requirements:

- I. Comply with the requirements of laws and regulations for the protection of personal information, customer contracts and other relevant regulations.
- II. To protect the personality rights of the parties to the personal information and to provide the legal autonomy of their personal information.
- III. The process of collecting, processing and using personal information shall be based on honesty and credit methods, and shall not exceed the necessary scope of specific purposes and shall have a legitimate and reasonable connection with the purpose of collection.
- IV. To provide appropriate security measures for personal information files to ensure that the Company is able to perform its duty of care for good management.
- V. To ensure the implementation extent of internal and external regulations and to determine the acceptable level of risk for personal information protection and responded measures;
- VI. 6. For the management of the personal information outsourced to third party , to ensure that the third party is responsible for the protection of personal information.

Article 5. Organizational Framework and Duties Related to the Management of Personal Information Protection

Personal information and management organization structure and duties shall be further established.

Chapter 3 Define the scope of personal information

Article 6. Personal Information Files

- I. Business Information Framework (BIF): Based on the business-oriented principle, analyze the personal information file and information flow, as well as the management status in order to present the overview of the personal information flow.
- II. Personal information file list: Refers to a list established according to the personal information file and information flow, as well as the management status.
- III. Personal information file group

| Group | Description of the group |
|---|--|
| High risk personal information | Containing special personal information: Personal information file containing medical records, medical treatment, genetic information, sexual life, health examination, and criminal records. |
| | Information of a nature that is relatively special, sensitive, or prone to be used to cause internal/external customer loss. Such as: credit card number, ID number, passport number, bank deposit/loan account number, unified identification number/alien resident certificate number for foreign nationals, other financial information or personal information files of minors and vulnerable adults. The age of abovementioned minors is defined based in Civil Law provisions; a vulnerable adult is defined as a person who is subject to the order of the commencement of guardianship or assistantship. |
| Personal information with general and direct identification | Except for high-risk personal information, files containing information for identifying a specific individual. Such as: name, net member account. |
| Personal information with indirect identification | Where the use of such information is insufficient for identification, and it is necessary to compare, combine or link, etc., with other information in order to identify the specific individual. Such as: date of birth, characteristics, marital status, family, education, occupation, social activities, contact information, discernible nationality, health insurance ID number, natural person certificate number, LINE UID, and insurance policy number |

Article 7. Personal information file checking

Each unit of the Company shall check the personal information file, identify its status, and establish a BIF and “Personal Information File List”. If the result of checking shows no personal information files, then there is no need to establish a BIF and “Personal Information File List”.

With the consideration that the personal information related to the information unit is stored in the system, consequently, after the checking of the personal information files, it is only necessary to establish the “Personal Information file Inventory List”.

Article 8. Personal information file list update

- I. The unit possessing the personal information files (i.e. the personal information management unit) shall check the process for inventory taking and update the BIF at least annually (excluding the information unit) and the “Personal Information File List”.
- II. For a unit without any personal information files after the checking result for the first time and the unit possessing the personal information files, when there is a major change in the personal information file or launch of new products or services, the responsible unit shall perform the process inventory taking and the checking of personal information files. In addition, the BIF and “Personal Information File List” shall be revised according to the inventory taking and checking result, which shall also be signed and approved by the unit supervisor.

Chapter 4 Personal information Risk Assessment

Article 9. Personal Information Management Impact Analysis

Personal information management impact analysis: Analyze the difference between the current personal information file control measures and various regulatory requirements for personal information protection.

Article 10. Timing of Personal Information Management Impact Analysis

After the unit possessing the personal information files completes the personal information file inventory taking, BIF, and personal information file list for the first time, it is necessary to perform personal information management impact analysis, which shall be performed periodically for subsequent years annually.

Article 11. Personal Information Protection Self-assessments

The personal information management shall perform self-assessment on the risk of the personal information possessed according to the “Fubon Financial Holding Co., Ltd. and Subsidiaries Personal Information Protection Self-assessment Management Guideline”, and shall periodically submit relevant self-assessment reports to the Operational Risk & Planning Department.

Article 12. Reporting of Personal Information Protection Management Information

The Company should review regularly the impact of internal and external issues pertaining to personal information file and the concerned parties’ expectation on personal information protection, to respond to relevant risks and to take action as early as possible. Any potentially important issues should be reported to the Personal Information Protection and Supervision Committee.

If there are major changes to the business, products, processes, and systems involving the personal information file, the responsible unit shall conduct risk assessment in accordance with internal regulations and incorporate personal information privacy protection into designing considerations before launching new business, products, process or systems.

The effective measuring indicators and cycles for the management objectives for personal information should be established to assure the implementation level of the objectives. For any indicators not reaching the objectives, improvements are required.

Chapter 5 Use Records, Trace Information, and Evidence Preservation

Article 13. **Preserving Records of Personal Information Use**

The personal information management unit shall prepare document records of personal information use status, preserve trace information of automatic machine equipment, or preserve relevant evidence in order to implement relevant personal information protection and management thoroughly.

The Company executing various types of personal information protection mechanisms, procedures, and measures specified in the Guideline shall record the personal information use status thereof and preserve the trace information or relevant evidence. Relevant trace information, evidence, and records shall be preserved for at least five years. However, where the law or contract specifies otherwise, such restriction shall not be applied.

Article 14. **Preserving Evidence of Personal Information Infringements**

In case of the occurrence of infringement on personal information, investigation activities shall be conducted in order to identify the cause and to distinguish personnel liability, thereby providing complete evidence during dispute handling and litigation proceedings. It is necessary to establish the personal information identification requirements, including evidence perpetuation and preservation, evidence recovery and reconstruction, evidence analysis and identification, etc.

Chapter 6 Overall Continuous Improvement for Personal Information Security Maintenance

Article 15. **Operating Framework of Personal Information Protection Management System**

The structure of the personal information protection management system shall be based on the “plan-do-check-act”, and the information security and relevant regulations of the Personal Information Protection Act shall be implemented during daily management and operation.

Article 16. **Ongoing Improvement of Personal Information Protection Management System**

According to the inspection and measurement results and recommendation of the preceding paragraph, execute corrective and preventive measures, Foran internal or external audit issues or an important personal information **incidents**, it should include a root cause identification procedure in order to continuously improve the personal information protection management system.

Chapter 7 Definition and Explanation

Article 17. Collection

Refers to collecting personal information in any form and way.

Article 18. Processing

Refers to recording, input, store, compile, correct, duplicate, retrieve, delete, output, connect or internally transmit information for the purpose of establishing or using a personal information files.

Article 19. Use

Refers to all methods of personal information use other than processing.

Chapter 8 Personal Information Collection

Article 20. Special Purposes of Personal Information Collection

The collection of personal information, except for the information specified in Paragraph 1 of Article 26 of the Guideline, shall have specific purposes, and shall comply with one of the following conditions:

- I. It is in accordance with law.
- II. There is a contractual or quasi-contractual relationship between the Parties, and proper security measures have been adopted.
- III. Where the Party has made public such information by himself or when the information has been publicized legally.
- IV. Consent has been given by the Party.
- V. It is necessary to promote public interests.
- VI. The personal information is obtained from publicly available resources. However, it is exempted if the information is limited by the Party on the processing or use and the interests of the Party shall be protected.
- VII. The rights and interests of the Party are not harmed.

The consent mentioned in Subparagraph 4 above means a declaration of intention made by the Party to allow the collection or processing of personal information after notification is given by the collector in accordance with the Personal Information Protection Act.

The Party's consent to provisions in Paragraph 1, Subparagraph 4 may be presumed if the Party does not indicate any refusal and also provides his/her personal information, when the Company gives express notice to the Party in accordance with Article 22 of the Guideline.

The collector shall have the burden of proving that the Party has given the consent under the Personal Information Protection Act.

At the time when the collector realizes or has been notified of the provision in Subparagraph 6 of Paragraph 1 by the Party, he/she shall delete, stop processing, or using the personal information, ex officio or upon the request of the Party.

Article 21. Regular Checks of Special Purposes of Personal Information Collection

When collecting personnel information for the Party, it is necessary to inspect whether its specific purpose complies with the criteria of the relevant laws, and it is necessary to periodically determine whether the specific purpose for preserving the personal information has diminished, or whether the

preservation period has expired annually, and shall also preserve confirmation trace records for submission to the supervisor for review and approval.

Article 22. Notification of Personal Information Collection

The following items shall be told precisely to the Party by the Company when collecting personal information from the Party:

- I. Name of the Company.
- II. Purpose of collection.
- III. Classification of the personal information.
- IV. Time period, area, target and way of the use of personal information.
- V. Rights of the Party and ways to exercise them as prescribed in Article 3 of the Personal Information Protection Act.
- VI. The influence on his/her rights and interests while the Party chooses not to provide his/her personal information.

Article 23. Exemption of Notification of Personal Information Collection

When collecting personal information of the Party, the following situations may be exempted from the notice prescribed in the preceding Paragraph:

- I. When in accordance with law.
- II. When the collection of personal information is necessary for the Company to fulfill the legal obligation.
- III. When the notice will impair the government agency in performing its official duties.
- IV. When the notice will impair public interests.
- V. When the Party should have known the content of the notification already.
- VI. When the collection of personal information is for non-profit purposes and clearly does not cause any detriment to the Party.

Article 24. Method of Notification of Personal Information Collection

Regarding the notice for the method of collecting personnel information from the Party, such method may be described in relevant notice section of contracts, application forms, notices, authorizations, etc. The content of notice shall be reviewed by the legal or legal compliance unit and shall also be approved according to the delegation of authority in order to confirm its appropriateness.

Article 25. Notification of Collection of the Personal Information of Minors or Vulnerable Adults

Statutory notices shall be executed according to the method of notice specified in the relevant laws and regulations of personal information protection, if the party is a minor or a vulnerable adult, the consent of the legal representative or guardian of the party must be obtained, and records of notice shall be preserved.

Article 26. Collection of Special Personal Information

During the collection of personal information, it is necessary to inspect whether the information collected contains special personal information. Personal information of medical records, medical treatments, genetic information, sexual life, health examination and criminal records shall not be collected, processed, or used. However, the following situations are not subject to the limits set

in the preceding sentence:

- I. When in accordance with law.
- II. When it is necessary for a company to fulfill its legal obligations, and proper security measures are adopted prior or subsequent to such collection, processing, or use.
- III. When the Party has made public such information by themselves or when the information concerned has been publicized legally.
- IV. Where it is necessary to assist a government agency in performing its legal duties or a non-government agency in fulfilling its legal obligations, and proper security measures are adopted prior or subsequent to such collection, processing, or use.
- V. Where the Party has consented in writing. Unless such consent exceeds the necessary scope of the specific purpose, the collection, processing or use merely with the consent of the Party is prohibited by other statutes, or such consent is against the Party's will.

Article 8 and Article 9 of the Personal Information Protection Act shall apply mutatis mutandis to the collection, processing, or use of personal information in accordance with the preceding Paragraph. Paragraphs 1, 2, and 4 of Article 7 of the Personal Information Protection Act shall apply mutatis mutandis to the written consent specified in Subparagraph 5 of the preceding Paragraph. The notification should be in written form.

Chapter 9 Personal Information Processing and Use

Article 27. **Notification of Indirect Collection of Personal Information**

The Company should notify the Party of the source of information and Subparagraphs 1 to 5 of Paragraph 1 of Article 8 of the Personal Information Protection Act, before processing or using personal information collected in accordance with Article 19 of the Personal Information Protection Act which was not provided by the Party.

The notification mentioned in the preceding Paragraph may not be given for the following:

- I. Under one of the situations listed in Article 23 of the Guideline.
- II. When the Party has made public such information by himself/herself or when the information has been publicized legally.
- III. When the notification may not be made to the Party or his legal representative;
- IV. When it is necessary for public interests on statistics or the purpose of academic research. The information may not be used to identify a specific person after a treatment of the provider or the disclosure of the collector;

The notification mentioned in Paragraph 1 may be undertaken when the personal information is used against the Party for the first time.

Article 28. **Special Purposes of Personal Information Processing**

The processing of personal information, except for the information specified in Paragraph 1 of Article 26 of the Guideline, should have specific purposes, and should comply with any one of the following conditions:

- I. It is in accordance with law.
- II. There is a contractual or quasi-contractual relationship between the Parties, and proper security measures have been adopted.

- III. The Party has made public such information by themselves or when the information has been publicized legally.
- IV. Consent has been given by the Party.
- V. It is necessary to promote public interests.
- VI. The personal information is obtained from publicly available resources. However, it is exempted if the information is limited by the Party on the processing or use and the interests of the Party should be protected.
- VII. The rights and interests of the Party are not harmed.

The consent mentioned in Subparagraph 4 above means a declaration of intention made by the Party to allow the collection or processing of personal information after notification is given by the collector in accordance with the Personal Information Protection Act.

The Party's consent to provisions in Paragraph 1, Subparagraph 4 may be presumed if the Party does not indicate any refusal and also provides his/her personal information, when the Company gives express notice to the Party in accordance with Article 22 of the Guideline.

For the processing of personal information, it is necessary to inspect whether its specific purpose satisfies the criteria of relevant laws.

At the time when the collector or processor realizes or has been notified of the provision in Subparagraph 6 of Paragraph 1 by the Party, he/she should delete, stop processing or using the personal information, ex officio or upon the request of the Party.

Article 29. **Principles Governing Collection, Processing, or Use of Personal Information**

The rights and interests of the Party should be respected in collecting, processing or using personal information and the information should be handled in accordance with the principle of bona fide. It should not go beyond the purpose of collection and should be reasonable and fair.

Article 30. **Security Measures Involved in the Collection or Use of Personal Information**

For the processing or using of personal information, proper security measures should be adopted to prevent the personal information from being stolen, altered, damaged, destroyed or disclosed, and necessary measures in terms of technology and organization should be adopted.

Article 31. **Providing Personal Information Files to Third Parties**

Where there is a need to provide personal information to a third party (such as: competent authority, certified public accountant, prosecution/police/investigation agency, taxation agency, court, etc.), a record shall be kept and shall be signed and approved by the supervisor.

Article 32. **Using Personal Information for Marketing Purposes**

In the event that a subsidiary uses personal information for marketing, when the Party refuses to accept such marketing, the use of his/her personal information for marketing shall be stopped immediately, and the personnel of the unit shall be informed. The measures of refusal at the first marketing action should be notified to the Party, and the necessary fees should be paid by the

subsidiary.

Article 33. Special Purposes for the Use of Personal Information

Except the information stated in Paragraph 1, Article 26 of the Guideline, the Company should use the personal information in accordance with the scope of the specific purpose of collection provided. However, the information may be used outside the scope upon the occurrence of one of the following conditions:

- I. It is in accordance with law.
- II. It is necessary for promotion public interests.
- III. It is to prevent harm on the life, body, freedom or property of the Party.
- IV. It is to prevent harm on the rights and interests of other people.
- V. Consent has been given by the Party.
- VI. Such use may benefit the Party.

The consent mentioned in Subparagraph 5 above means a separate declaration of intention made by the Party to allow the use of personal information after the collector has expressly notified the Party of the purpose other than the originally-specified purpose, and the scope of use, and also the impact of whether consent is given or not on the Party's rights and interests.

For the use of personal information, it is necessary to inspect whether its specific purpose satisfies the criteria of relevant laws.

Article 34. Control of use of personal information for purposes other than the originally-specified purpose

- I. For the use of personal information for purposes other than originally-specified purpose, the written consent of the supervisor shall be obtained in advance.
- II. After the written consent of the supervisor, if it is necessary to obtain the written consent of the Party, the Party shall be informed of the purpose other than the originally-specified purpose, and the scope of use, and also the impact of whether consent is given or not on his/her rights and interests. In addition, the Party shall be requested to sign an agreement.
- III. Personal information used for purposes other than the originally-specified purpose shall be updated in the personal information file inventory list.

Article 35. **Processing and Use of Special Personal Information**

For the processing or using of special personal information of medical records, medical treatment, genetic information, sexual life, health examination and criminal records that are of high confidentiality and sensitivity, appropriate security protection measures should be provided before and after such process and use thereof.

Article 36. **International Transmissions of Personal Information**

International transmission of personal information should not involve major national interests and should not be made through an indirect method through a third country (region) to avoid the provisions of the Personal Information Protection Act, and should not violate international treaties or agreements specified otherwise. In case the country receiving the personal information lacks proper regulations towards the protection of personal information such that it might harm the

rights and interests of the Party, then no international transmission shall be made. Prior to performing international transmission of personal information, it is necessary to inspect whether it is subject to restrictions of the Financial Supervisory Commission (FSC) and shall comply with its regulations.

Article 37. **When Special Purpose for Collection of Personal Information no Longer Exists or Deadline Expires**

The information collected should be deleted, discontinued to process or use, ex officio or upon the request of the Party when the specific purpose no longer exists or the time period expires (however, the preceding sentence may not be applicable when it is necessary for the performance of an official duty or fulfillment of a legal obligation and has been recorded, or when it is agreed by the Party in writing), and the following records should be preserved:

- (I) The method of deletion, discontinued processing or use, and time thereof.
- (II) When the personal information that is deleted, discontinued from processing or use is transferred to other parties, the reasons, parties, methods, time of such transfer, and the legal basis for the collection, processing, or use for such parties.

The trace information, evidence, and records described in the preceding paragraph shall be preserved for at least five years. However, where the law or contract specifies otherwise, such restriction shall not be applied.

Article 38. **Handling Violations in the Collection, Processing or Use of Personal Information**

The information collected should be deleted, discontinued to process or use, ex officio or upon the request of the Party in cases where a violation of this Law occurred during collecting, processing or using that information.

Chapter 10 Commissioned Collection, Processing, and Use of Personal Information

Article 39. **Commissioning the Collection, Processing, and Use of Personal Information**

An agency commissioned to collect, process, or use personal information (hereinafter referred to as the “commissioned agency”) shall be considered the commissioning agency within the scope of the Personal Information Protection Act. The commissioning agency shall properly supervise the commissioned agency, and the supervision shall include at least the following:

- I. The planned scope, classification, specific purpose and time period of collecting, processing, or using personal information.
- II. The commissioned agency shall only perform the collection, processing or use of the personal information within the scope instructed by the commissioning agency. If it is considered that the commissioning agency’s instructions violate the Personal Information Protection Act, other personal information protection-related laws or their regulations, the commissioned agency shall notify the commissioning agency immediately.
- III. For the necessary security measures adopted by the commissioned agency to prevent the personal information from being stolen, altered, damaged, destroyed or disclosed in terms of technology and organization, such standards shall not be inferior to the requirements specified in the Personal Information Protection Act and the Enforcement Rules thereof.
- IV. When the commissioned agency or its employees violate the Personal Information Protection Act, other personal information protection-related laws or their regulations, the

commissioned agency shall notify the commissioning agency immediately and remedial measures shall be taken.

- V. When the commissioning relationship is terminated or rescinded, the commissioned agency shall return the carriers of the personal information and shall delete or destroy the personal information possessed by the commissioned agency with the storage method specified in the commissioning agreement, and affidavit or relevant proofs shall be issued for such matters.

In case the commissioned party or its employees or sub-commissioned party violate the aforementioned supervision requirements specified, such that the Company suffers damages or losses, the commissioning agency shall indemnify or compensate the Company, and its scope shall include but not be limited to the attorney's fee incurred and reputation damage for the claim made by a third party.

Article 40. **Contracts for Commissioning the Collection, Processing, and Use of Personal Information**

In addition to the required matters to be included in a commissioning contract as specified in the “Regulations Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operation” of the competent authority, the relevant supervision and responsibilities of the commissioned agency described in the preceding paragraph shall also be included in the commissioning contract in order to request to the commissioned agency to comply with such requirements.

Article 41. **Supervision of Commissioned Agency**

When commissioning others to collect, process, or use personal information, the commissioning agency shall properly supervise the commissioned agency. For any further sub-commissioning, its supervision shall be under the commissioned agency.

Article 42. **Verification of Commissioned Agency’s Protection of Personal Information**

The commissioning agency shall periodically verify the implementation status of the personal information protection measures by the commissioned agency, and shall record the result thereof for submission to the supervisor for review and approval.

Chapter 11 Procedures for claiming and exercising party’s rights

Article 43. **Party’s Rights**

Rights of the Party: Refers to the rights exercisable by the Party on his/her personal information according to the Personal Information Protection Act, and such rights include inquiry, request for a review, request to make duplications, request to supplement or correct, request to discontinue collection, processing or use of personal information.

The aforementioned rights should not be waived in advance or limited by a specific agreement.

Article 44. **The Party**

The Party: Refers to means an individual of whom the personal information has been collected, processed or used in accordance with the Personal Information Protection Act .

Chapter 12 Acceptance of exercise of the Party's rights

Article 45. Acceptance of the Exercise of the Party's Rights

The unit possessing the personal information files and having business dealings with customers directly shall establish an acceptance window for the exercise of the Party's rights.

Article 46. Recording Acceptance of the Exercise of the Party's Rights

The acceptance of the exercise of the Party's rights shall be recorded.

Article 47. Verifying Identity of Party Exercising His or Her Rights

For the acceptance of the exercise of the Party's rights, the identity of the Party shall be verified. In case of any inconsistency, his or her request shall not be accepted. In addition, the methods for the exercise of the Party's rights shall be provided and shall inform the Party about the required fee payment and provide the necessary explanation.

If the party referred to in the preceding paragraph is a minor or a vulnerable adult, in addition to confirming the identity of the party, it shall also confirm the identity of the legal representative or guardian of the party, and shall obtain the consent of the legal representative or guardian of the party to protect the party's privacy and right.

Article 48. Verification of Information on Party's Application

To ensure the correctness and reasonableness of the application, the personal information item applied and the information possessed by the Company shall be verified to be consistent.

Article 49. Approval/Disapproval of the Exercise of the Party's rights

- I. In case of any one of the following conditions, the Company may refuse the application of inquiry, review, or making of duplications of personal information:
 - (I) Where the national security, diplomatic and military secrets, macro-economic interests, or other major national interests may be harmed.
 - (II) Where the performance of official duties may be interfered with.
 - (III) Where the major interests of the Company or a third person may be affected.
- II. In case of any one of the following conditions, the Party's application for deletion, discontinued process, or use of personal information may be rejected:
 - (I) Where it is specified in the laws and regulations.
 - (II) Where it has not reached the preservation period specified in the contract.
 - (III) Sufficient reasons to consider that such deletion will affect the Party's interests which are worthy of protection.
 - (IV) Other justifications not to delete.
- III. When the Party requests an inquiry, review or making of duplications of personal information, the Company should determine within fifteen days for approval or disapproval. It may be extended to a time period of no longer than fifteen days when necessary and the Party should be notified of the reason thereof in writing.

- IV. When the Party requests a supplement, correction, deletion and discontinued collection, processing or use of personal information, the Company should determine for approval or disapproval within thirty days. It may be extended to a time period of no longer than thirty days when necessary and the Party should be notified of the reason thereof in writing.

Article 50. **Acceptance of the exercise of the Party's rights for inquiry, review, or making of duplications of personal information**

- I. The Company shall prepare application forms for the exercise of the Party's rights for inquiry, review, or making of duplications according to the business characteristics, or shall incorporate the content of the Party's request into existing application forms. The aforementioned application forms shall be reviewed by the legal or legal compliance unit and shall be approved according to the delegation authority in order to allow the Party to exercise his/her rights.
- II. When the exercise of the Party's rights for inquiry, review, or making duplications of his/her personal information involve different units, the Party shall complete an application form, and after the acceptance window verifies the identity of the Party to be correct without errors, the application form is then submitted to the relevant responsible unit for handling.
- III. When the Party requests an inquiry, review or making duplications of personal information, the necessary costs and charges may be collected.

Article 51. **Acceptance of the exercise of the Party's rights for supplement, correction, or request for deletion, discontinued collection, processing and use of personal information**

- I. The accuracy of the personal information shall be maintained, and it shall be corrected or supplemented actively or according to the request of the Party.
- II. When the Party proceeds to the business location to apply for the supplement or correction of his/her personal information, it is necessary to complete an application form and this shall be approved by the supervisor.
- III. When the Party applies for deletion, discontinued collection, processing and use of his/her personal information, it is necessary to complete an application form and this shall be approved by the supervisor.
- IV. Where there is a dispute on the accuracy of the personal information, the Company shall actively stop the processing or use of the personal information or shall stop such processing or use according to the request of the Party. However, where it is necessary for the performance of duties or business, or where the written consent of the Party is obtained and the dispute is indicated, then such restriction may not be applied.

Chapter 13 Handling and Response to Exercise of the Party's Rights

Article 52. **Providing Duplicates of Personal Information**

The duplication of personal information provided to the Party shall be consistent with the internal information of the Company. After the second review of the supervisor and the confirmation of the identity, it shall be provided to the Party in an encrypted or document sealed method, and a

copy shall also be retained or other proof documents capable of presenting the original shall be retained, along with the signing receipt record of the Party or other methods capable of confirming the serve to the Party.

Article 53. Correcting or Supplementing Personal Information

If there are matters attributable to the Company such that personal information is not corrected or supplemented, it shall be corrected and supplemented, followed by informing the parties to which the personal information has been provided for use.

Article 54. Deleting Personal Information or Discontinuing Its Collection, Processing and Use

When the Party requests discontinued collection, processing use or deletion of personal information, the responsible unit shall review the “personal information file inventory list”, and shall confirm the request contents of the Party and the business dealings between the Party and the Company, such that after the approval of the supervisor, the collection, processing, use or deletion of personal information may be stopped, and audit traces and records of notices to the Party shall be preserved

Article 55. Tracking the Handling of the Party’s Exercising of His or Her Rights

The acceptance window shall periodically track the status of handling and response of the exercise of the Party’s rights, and shall submit these to the supervisor for review and approval.

Article 56. The Party’s Filing of a Complaint in a Dispute

When the Company refuses the request of the Party or where a dispute occurs, the Company shall provide the complaint filing channel and contact method to the Party, and shall prepare records (including the reason for rejection and the method of notice to the Party).

Chapter 14 Personnel Management

Article 57. Personal Information Protection Security Management Measures

The Company shall adopt security management measures according to the factors of the nature of the business, business process, personal information access environment, scope of personal information, personal information transmission tools and method, etc.

Article 58. Personnel Management Measures

The Company shall adopt the following personnel management measures:

- I. Establish different authorities for employees and control thereof according to the necessary job function segregation, responsibility allocation, authority management and operation, and determine the appropriateness and necessity of the setting of the authority content periodically. In addition, the authority of the relevant personnel accessing the personal information shall be established according to the necessity of job duties and the access status thereof shall be controlled.
- II. Employees shall bear the non-disclosure obligation.
- III. During the recruitment of personnel, it is necessary to request personnel to complete the

non-disclosure declaration. During the resignation, the personnel's identification code shall be canceled, and the access badges, cards, and relevant company identifications shall be recollected.

- IV. Each unit shall assign personnel to be responsible for the management of personal information files and account authorities. In case of a change of personnel job duties, handover procedures shall be performed, and their authorities shall be adjusted.
- V. The screen protection program activation time shall be set up. Prior to leaving one's seat, personnel shall log out of their computer or shall lock the screen.
- VI. Prior to leaving work, personnel shall shut down or log out of their computers, and notebook computers shall be locked or stored in locked cabinets.
- VII. Prior to leaving a conference room, the texts on the whiteboard shall be erased, and the meeting documents and files shall be removed.

Chapter 15 Operation Management

Article 59. **Management Measures for Personal Information Files**

The Company shall adopt operation management measures listed in each clause of this chapter for personal information:

Article 60. **Controlling the Transmission of Personal Information**

During the transmission of personal information, depending upon different transmission methods, it is necessary to determine whether there is a need for encryption. If it is considered necessary, an appropriate encryption or protection mechanism shall be adopted, and the correctness of the recipient of the information shall be confirmed.

- I. Transmission of personal information in physical papers
 - (I) For personal information files containing high-risk personal information and general direct personal identification, regardless of whether it is an internal Company transmission or transmission to the external of the Company, the personal information shall be properly sealed, and the addition of watermarks or other appropriate control methods to protect the personal information shall be considered.
 - (II) For personal information files containing special personal information, the transmission method confirmed to serve to the recipient shall be adopted.
- II. Transmission of electronic personal information
 - (I) Where personal information files are stored in cassettes, optical disks, or portable or external storage mediums, such files shall be encrypted or protected with other appropriate control methods, and shall be transmitted by a dedicated person, and a signing receipt mechanism shall be established.
 - (II) For personal information files containing high-risk personal information and general direct personal identification, regardless of whether it is an internal Company transmission or transmission outside the Company, important information shall be encrypted or protected with other appropriate control methods (such as a direct line or compression file with passwords, etc.)

- (III) The transmission of electronic files may be subject to rules in the information system for filtering electronic files containing personal information in real time. The setting or revision of these rules on filtering personal information shall be submitted to the president of the company concerned for approval before being carried out by the unit responsible for the company's information system. The company's unit responsible for the information system's personal information filtering rules shall check the appropriateness of the existing rules on an annual basis. If the unit determines that no revisions are needed, the unit's manager is authorized to approve the determination and then notify the company's unit responsible for the information system. The rules shall be kept confidential except when cooperating with audits or reviews or other actions necessary for business operations.
- (IV) Once the filtering rules for personal information are activated, the information system can be set to "transmit after review and approval," "transmission rejected," or "transmission permitted," depending on the nature of the business.
- (V) If there is a need to adopt a special processing method because of the needs of the business, it can be adopted after receiving the approval of the president of the company concerned. That means that if the transmission of an electronic file triggers the filtering rules for personal information, the information system will not block it.

Article 61. Management Measures for the Preservation of Personal Information Files

The following management measure for the preservation of personal information files shall be adopted.

- I. Preservation of personal information in physical papers
 - (I) For personal information files not processed via computer, dedicated personnel or a dedicated unit shall be designated for the management thereof in order to establish the mechanisms of file classification sorting, updates and borrowing/lending for review, etc.
 - (II) A physical paper control mechanism shall be established in order to ensure the proper preservation and integrity of personal information files. If it is necessary to use sealed boxes for preservation, an appropriate labeling mechanism shall be adopted. However, the labeling shall not disclose excessive information. The Company shall be aware of the moisture resistance and fire resistance of the physical paper preservation environment in order to ensure the safety and availability of the physical paper documents.
 - (III) Personal information files containing high risk personal information and general direct personal identification shall be preserved in a locked cabinet or a location with access control at all times.
 - (IV) Prior to leaving work, personnel shall store the personal information files in physical papers in a locked cabinet or a location with access control.
 - (V) The Company shall establish a personal information file preservation period. Where the law specifies the requirements, the preservation period shall not be less than the regulatory requirements. In addition, unless there are special reasons, in principle, the preservation period of personal information files shall not be set for permanent preservation.
 - (VI) For output equipment of printers, photocopy machines, fax machines or scanners, etc., passwords or other appropriate control methods shall be established. For the

printing, photocopying, or faxing of personal information containing high risk personal information and general direct personal identification, such personal information files shall be retrieved immediately, and the original documents shall be removed in order to prevent the leakage of personal information. Documents which are not retrieved shall be periodically collected and preserved properly by dedicated personnel, and a logbook shall be set up for registration. In addition, after the review and approval of the supervisor, if such documents are still not yet retrieved by any one exceeding three days, such documents shall be destroyed immediately.

- (VII) For paper documents containing personal information, an appropriate access mechanism shall be established.
- II. Preservation of electronic personal information files (including magnetic disks, cassettes, optical disks, telephone chips, computers, host computer equipment or other medium)
- (I) For personal information files processed via computers, dedicated personnel or dedicated unit shall be designated for management in order to establish a redundancy system, and a control mechanism for assessing control during the file creation, use, update, correction or deletion of such files shall be established.
 - (II) For preserved personal information content, appropriate protection control (such as: encryption: setting of opening passwords, etc.) shall be adopted.
 - (III) For backup data of personal information, appropriate protection controls (such as: encryption: access control, etc.) shall be adopted. The storage medium of backup data shall also be preserved with an appropriate method, and periodical backup of data sampling testing shall be performed in order to ensure the effectiveness of backing up data.
 - (IV) The Company shall establish preservation periods for various types of files. Where the law specifies requirements, the preservation period shall not be less than the regulatory requirements. In addition, unless there are special reasons, in principle, temporary personal information saved in personal computers shall be deleted immediately after use.
 - (V) All business requests shall be approved by the supervisor, and personal information shall not be saved in public folders or public computers.
 - (VI) The information unit shall establish relevant controls, and protection mechanisms shall be established.
 - (VII) The information unit shall perform monitoring on the technology environment and shall implement defense and handling for specific external attacks.
 - (VIII) The information unit shall adopt necessary protection, monitoring and record preservation measures depending upon the information and system security in order to detect and prevent computer viruses, other malware, or malicious actions, thereby preventing computer systems from hacking, damage, alteration and deletion.

Article 62. **Management Measures for the Destruction of Personal Information Files**

The destruction of personal information files shall adopt the following management measures:

- I. The destruction of personal information files shall be approved by the supervisor in advance, and shall be handled by more than two personnel (inclusive) at the same time. In addition, the information of the destruction date, content, quantity, destruction method, personnel

executing the destruction, etc., shall be recorded and submitted to the supervisor for review and approval.

- II. Prior to the discarding of a medium or information stored with the personal information or transfer thereof to others, the data stored in the medium shall be deleted properly according to the preceding paragraph, or shall be destroyed with a physical method. If there are backup files, such files shall also be deleted.
- III. When the Party requests the deletion of personal information files, if there are reasons sufficient to determine that the deletion will harm the interests of the Party and ought to be protected or there are proper reasons to not delete such information, according to the preservation period specified by the laws or the contract terms, then the Company shall stop the processing or using methods for deletion of the personal information on the Party's behalf.

Chapter 16 Information Equipment Management

Article 63. **Management of the Use of Information Equipment for the Collection, Processing or Use of Personal Information**

During the collection, processing, or use of personal information via information equipment, the following technical management measures shall be adopted:

- I. A verification mechanism shall be established on the information equipment in order to perform identification and control on personnel with authority to access personal information. During the change of personnel, the use authorities of such personnel shall be updated immediately.
- II. When the verification mechanism adopts the method of an account and password for verification, a quality password shall be used and periodic changing of the password shall be implemented.
- III. Unauthorized accesses shall be rejected, and warnings, as well as a relevant responsive mechanism, shall be set up. For unauthorized accesses, an audit trace shall be preserved and subsequent auditing shall be enhanced for tracking.
- IV. For terminals accessing personal information, account and password verification shall be performed, which shall also be identified and controlled.
- V. The quantity and scope of personal information access authorities shall be set up within the limit of necessary operations, and personnel shall not share identification accounts and passwords with others.
- VI. Supervisors shall approve the authority of users to access personal information application program in advance.
- VII. Each unit shall periodically inspect the reasonableness of its account and authority, and shall preserve traces for submission to the supervisor for review and approval.
- VIII. Anti-virus software shall be installed on the computer system processing personal information, and shall update the virus code periodically.

- IX. For any vulnerabilities of the computer operating system and relevant application programs, supplemental/updated programs shall be installed periodically.
- X. The threats of malware shall be understood periodically, and the stability of the computer system after the installation of anti-virus software and supplemental/updated programs shall be determined.
- XI. Personal computers shall not install file sharing software.
- XII. Under the testing environment, real personal information shall not be used. In case real personal information is used, such information shall be masked or altered.
- XIII. If there is any change in the information system processing personal information, its security shall be determined to have not been reduced.
- XIV. The rules for use of various types of equipment and storage mediums shall be established, and when the equipment or medium is scrapped or used for other purposes, appropriate measures shall be adopted to prevent the leakage of information.
- XV. During the use of computers and relevant equipment to process personal information, rules for the use of portable storage mediums shall be established.
- XVI. The passwords used in the verification mechanism and encryption mechanism shall be properly preserved, and a password handover procedure shall be established.
- XVII. For the preserved personal information content, where there is a need for encryption, appropriate encryption measures shall be adopted during the collection, processing, or use thereof.
- XVIII. Personal information files duplicated and backed up shall be equipped with appropriate protective measures.
- XIX. Personal mobile devices or equipment (such as mobile phones, cameras, and notebooks) must not be used for capturing or storing a customer's personal information.

Article 64. **Required security measures for the e-commerce service system**

For the e-commerce service system, the following information security measures shall be adopted:

- I. User identification confirmation and protection mechanism.
- II. Code masking mechanism for display of personal information.
- III. Safety encryption mechanism of internet network transmission.
- IV. Software verification and confirmation procedures for each stage of development, online and maintenance of application system.
- V. Access control and protection monitoring measures for personal information files and database.
- VI. Strategies to prevent intrusion from an external network.

VII. Monitoring of illegal or abnormal use actions and responsive mechanisms.

The term of “e-commerce” described in the preceding paragraph refers to various commercial trading activities related to advertisement, marketing, supply, purchase or delivery, etc., of products or services through the internet.

The “code masking mechanism for display of personal information” specified in Subparagraph 2 of Paragraph 1 refers to the effect of removing identification through masking codes under the condition where the normal transaction information display is not affected. Where the e-commerce service system has performed effective identification on the identity of the customer, for the purpose of determining the necessity of the transaction and ensuring the accuracy as well as the verification information that is obtained, the information of inward (outward) account transfer, transaction amount, account balance and notes, etc., displayed on the system shall not adopt the aforementioned code masking mechanism. However, to protect the security of customers’ personal information, the e-commerce service system shall still use the identification removal with code masking method as much as possible for the personal information displayed or printed during the transaction process under the condition where the aforementioned purpose is not affected.

The measures specified in Subparagraphs 6 and 7 of Paragraph 1 shall be periodically rehearsed, reviewed, and improved.

Chapter 17 Physical Environment Security

Article 65. **Protecting Stored Physical Personal Information Files**

For locations stored with physical files of personal information, or storage hosting machine, peripheral equipment and relevant facilities, protection against natural disasters and other accidents shall be enhanced, and crisis handling countermeasures and a reporting mechanism shall be established.

Article 66. **Maintaining the Physical Security of Personal Information Files**

To maintain the physical security of personal information files, employees of the Company shall comply with the “Fubon Financial Holding Co., Ltd. and Subsidiary Access Security Management Guidelines”.

Article 67. **Managing Areas Where Personal Information Files Are Stored**

For the dedicated areas equipped with computer equipment for storing personal information files and stored with personal information files, access control and physical security protection measures (such as surveillance, window opening sensors, etc.) shall be established.

Article 68. **Managing Office Areas**

During access to the area, employees shall be aware of preventing any suspicious persons from entering the office area without authorization, and shall also be aware of whether there is any suspicious person in the office environment.

Article 69. **Access Management for Archive Rooms, Warehouses**

The archive room or warehouse in the office shall be implemented with necessary access

management.

Article 70. **Disaster Prevention Equipment for Operating Areas**

For different operating environments, necessary disaster preventive equipment shall be installed.

Chapter 18 Prevention of personal information incidents

Article 71. **Preventing Personal Information Incidents**

For daily management and operation, the “plan-do-check-act” shall be used as the basis for implementing relevant regulations of information security and Personal Information Protection Act, in order to prevent security incidents of stealing, alteration, damage, loss or leakage, etc., of personal information (hereinafter referred to as the “incidents”).

Article 72. **Personal Information File Impact Analysis**

Through the impact analysis of personal information files, identify potential and nonconforming risks, and establish improvement measures in order to prevent personal information incidents.

Chapter 19 Reporting of Personal Information Incidents

Article 73. **Important and General Personal Information Incidents**

The unit which experiences the incident shall determine an incident to be a general or important personal information incident according to the following criteria:

- I. Important personal information incident: An incident that satisfies one of the following criteria shall be determined to be an important personal information incident.
 - (I) According to the evaluation of the unit which experiences the incident, the incident is subject to the likelihood of causing major damage to the reputation affecting the sound operation of the Company;
 - (II) Where a notice from the central competent authority for the business objective, judicial agency, or relevant government agency is received;
 - (III) Where a notice from a consumer protection organization is received;
 - (IV) Where a notice from the media is received or has been disclosed in the media;
 - (V) Where there is a likelihood of causing harm to the rights of more than 10 Parties (inclusive) due to one identical reason or fact;
 - (VI) Where the Party files a damage indemnification amount due to one identical reason or fact and the Company evaluates that such amount has reached the important operating risk event estimation loss amount threshold.

II. General personal information incident

A non-important personal information incident is considered as a general personal information incident.

Article 74. **Notification of Personal Information Incidents**

When the unit which experiences the incident determines that there is a possibility of the

occurrence of a personal information incident, it shall report according to the “Fubon Financial Holding Co., Ltd. Operational Risk Reporting and Management Guideline” or relevant regulations of the Company.

Article 75. **Notification of Major Personal Information Incidents**

When a unit experiences a major personal information incident as defined by the FSC:

I. The unit that experienced the incident shall report it based on reporting guidelines for major operational risk events and “Fubon Financial Holding Co., Ltd. and Subsidiaries Guidelines for Reporting Major Events to Regulatory Authorities.” It shall also fill out a “Personal Information Infringement Incident Reporting Form” (see Attachment 1) on the day the personal information leak is discovered and submit it to the Operational Risk & Planning Department.

II. After the Operational Risk & Planning Department completes its review process, it must quickly hand over the case to the Audit Division, which shall fill out a “Personal Information Infringement Incident Reporting and Recording Form” (Attachment 2) within 72 hours after the personal information leak was discovered and submit it to the FSC. If other related laws and regulations exist, however, the case shall be handled according to those provisions. The corrective and preventive measures established in response shall be analyzed and reviewed by fair and independent experts who have relevant publicly recognized qualifications.

The major personal information incidents referred to above refer to personal information being stolen, altered, damaged, lost or leaked in a way that threatens the normal operations of the Company or the rights and interests of large numbers of data subjects.

Chapter 20 Responsive Mechanism for General Personal Information Incidents

Article 76. **Investigations and Notifications of Personal Information Incidents**

The unit which experiences the incident shall investigate the authenticity of the incident, the quantity and scope of information subject to stealing, leakage, etc., and shall also perform digital evidence and paper evidence in order to facilitate the producing of evidence for legal aspects. For an incident determined to be a personal information incident, after the internal signing approval, a statutory notice shall be performed according to the method of notice specified in the personal information protection-related laws and regulations, and shall also preserve the record of notice. The content of notice to the Party shall include the fact of the infringement of personal information and the responsive measures already adopted, as well as the consultation service direct line, in order to allow the Party to understand the relevant status, and to provide a subsequent inquiry and assistance.

Article 77. **Personal Information Incident Responses and Corrective Measures**

In case of a personal information incident caused by matters attributable to the Company, responsive measures shall be adopted, including the method for controlling the damage of the Party, in order to reduce or control the scope of damage, and to establish improvement measures, thereby preventing re-occurrence of incident.

Chapter 21 Responsive Mechanism for Important Personal Information Incident specified by the Company or Major Personal Information Incident specified by the FSC (hereinafter referred to as the “important personal information incident and major personal information incident)

Article 78. Personal Information Emergency Response Team

To cope with the handling of important or major personal information incidents, the Company shall establish a personal information emergency response team, and the team members shall include the personal information incident response team convener, function units for the occurrence of incidents, incident management, information, public relationship and media, audits, and legal or legal compliance units, etc. When an incident is determined to be important or a major personal information incident by the unit which experiences the incident, it shall inform the incident management unit and the personal information emergency incident response team convener.

Article 79. Convening a Meeting of the Personal Information Emergency Response Team

When the personal information emergency response team convener is informed of an important or major personal information incident, he or she may convene the personal information emergency response team meeting depending upon the impact level and severity of the personal information incident in order to lead the emergency responsive action, to manage the incident information and to perform decision making. After the completion of the handling of important or major personal information incidents, an incident review meeting shall be convened in order to discuss and establish corrective and preventive measures in order to correct and prevent such type of incident.

Article 80. Handling a Personal Information Incident

The unit which experiences the incident shall investigate the authenticity of the incident, the quantity and scope of information subject to stealing, leakage, etc., and shall also perform digital evidence and paper evidence in order to facilitate the producing of evidence from legal aspects. For an incident determined to be a personal information incident, in addition to the control of the damage of the Party, after the internal signing approval, a statutory notice shall be performed according to the method of notice specified in the personal information protection-related laws and regulations, and shall also preserve the record of notice. The content of notice to the Party shall include the fact of the infringement of personal information and the responsive measures already adopted, as well as the consultation service direct line, in order to allow the Party to understand the relevant status, and to provide subsequent inquiry and assistance.

Article 81. Responsibilities of Incident Management Unit

When an incident management unit receives the report on an important or major personal information incident, it shall inform the personal information emergency response team convener, assist the convener to convene the meeting, and coordinate as well as track the improvement measures.

Article 82. Collection of Digital Evidence

Where the personal information incident is related to the information system, the information unit shall assist the unit which experiences the incident to perform digital evidence collection to

facilitate the providing of evidence from legal aspects, and to investigate the root cause as well as to perform review and improvement.

Article 83. Handling a Media Crisis

The public relationship unit shall monitor the media reports, and shall announce written statements to the external according to the “Fubon Financial Holding Co., Ltd. and Subsidiary Principles for Media Crisis Management”, and shall communicate with the internal employees. In addition, the customer service unit shall assist in communication with the consumer protection organization and handle the Q&A for customers.

Article 84. Notifying Competent Authorities

Where an incident complies with the reporting standard or major personal information incident according to the “Fubon Financial Holding Co., Ltd. and Subsidiaries Guidelines for Reporting Major Events to Regulatory Authorities”, then a report to the central competent authority for the business objective shall be made according to the requirements specified in these Guidelines.

Article 85. Responsibilities of Legal or Compliance Unit

The legal or legal compliance unit shall assist relevant units in understanding whether the incident violates the personal information protection-related laws and regulations, and shall provide legal consultation services depending upon the needs.

Chapter 22 Personal Information Handling Procedures after the Termination of Business

Article 86. Personal Information Handling Procedures after the Termination of Business

These procedures are applicable to the business department and business related department in the personal information protection management system in order to specify how to appropriately handle the personal information files for such business after the termination of the business.

Article 87. Termination of business

Refers to the Company eliminates all or a portion of a continuing contract relationship between the Party and the Company for future business, and it may include the conditions: termination of existing portion of business of the Company, merger action of the Company, liquidation and dissolution of the Company, etc.

Chapter 23 Personal Information Files Management after Termination of Business

Article 88. Procedures to Follow in a Business Transfer

Where a portion or all of the business is transferred to another company, the following procedures shall be complied with.

- I. Inventory taking on the relevant personal information files related to such termination of business shall be made, and an inventory list shall be created for management thereof.
- II. Perform the personal information file handover procedure according to the personal information file inventory list. The handover procedure shall be handled by the business

unit. In addition, the handover person, takeover person, and supervision person shall be present onsite to perform the handover procedure. After the personal information file handover procedure is completed, the handover person, takeover person and supervision person shall jointly sign on the handover inventory list. The handover inventory list shall at least include the reason, subject, method, time, location of the transfer, as well as the legal basis and proof for the transfer subject to retain such personal information files, which shall be made in two original copies for the handover person and takeover person to retain one copy each.

III. Prior to the transfer, the contract relationship transfer requirements for the contract between the Company and the Party shall be determined first.

If the contract relationship specifies that the Company may transfer the personal information collected, processed, and used after informing the Party, then the Company may transfer the personal information after informing the Party without obtaining the written consent of the Party in advance.

If the transfer of the contract relationship is not specified as described above, then according to the regulations of the Civil Code, the transfer of the contract relationship shall be executed based on the consent of the Party. After the consent of the Party, and after the Company has explicitly informed the Party about the reason, subject, method, time, location of the transfer, as well as the legal basis and proof for the transfer subject to retain such personal information files, the personal information can then be transferred to the transferee.

IV. Where the Party disagrees with the transfer of the contract relationship, the Company shall assist the Party to perform the cancellation of the contract relationship, or shall delete his/her personal information of the Party without transferring the personal information to the transferee.

Article 89. **Procedures to Follow after a Business Termination**

For the termination of a portion or all of the business, the following procedures shall be complied.

- I. Inventory taking on the relevant personal information files related to such termination of business shall be made, and an inventory list shall be created for management thereof.
- II. Prior to the termination of business, the Company shall actively inform the Party, following which the personal information files preserved may then be deleted. If the Party raises objections, subsequent handling of the personal information files may then be performed according to the request of the Party.

Article 90. **Destruction or Transfer of Files**

For the destruction or transfer of personal information files, records related to the destruction or transfer shall be retained according to the preservation period specified by the law and internal regulations.

Chapter 24 **Personal Information Protection and Management Educational Training**

Article 91. **Educational Training**

The human resources unit shall implement the “Educational Training for Knowledge of Response to and Impact of Personal Information Protection Act” on the Financial Holding and subsidiaries/sub-subsidiaries through E-Learning or other methods annually, and records shall be

preserved. For new employees, the educational training of the Personal Information Protection Act is incorporated into the new employee orientation course.

Article 92. **Planning Educational Training Based on Business Needs**

To allow personnel (including regular or irregular contract personnel of the Company) required to access personal information during the execution process of job duties to understand the requirements of personal information protection-related laws, the importance of personal information protection management, required responsibility for the use of personal information, impact of violations of personal information protection management on the Company and perpetrator, various types of personal information protection mechanisms, procedures, measures and implementation of non-disclosure obligation on the information of customers, the Company shall plan the annual personal information protection and management educational training according to the nature of business, and traces shall be preserved.

Article 93. **Reviewing Content of Educational Training Courses**

To cope with the change of the business environment of the Company, as well as the change of laws and regulations, the appropriateness of the personal information protection and management educational training content shall be reviewed at least annually.

Chapter 25 Audit and Improvement Procedures

Article 94. **Internal Audits and Internal Self-inspections**

The management mechanism of the Guideline shall be incorporated into the scope of internal audits and internal self-inspection in order to examine the effectiveness and implementation status of the Guideline.

Article 95. **Tracking and Correcting Deficiencies Found in Internal Audits and Self-inspections**

For the deficiencies found during the internal audit and internal self-inspection, the business unit shall enhance the improvement and establish preventive measures, and shall perform tracking until the improvement is complete.

Chapter 26 Others

Article 96. **Decision-making Authority**

The signing approval, approval, review or written consent of the supervisor described in the Guideline shall be executed according to the internal delegation of authority of each unit.

Article 97. **Management Exceptions**

When the requirements of the Guideline cannot be satisfied due to the nature of the business or cost concerns, the acceptable risk level shall be assessed first, and relevant remedy measures shall be planned. Under the premises where personal information protection-related laws and regulations are complied with, a report submission method may be made for submission to the President of the company in order to obtain approval for exceptions.

Article 98. Developing Detailed Rules

Each unit may establish more detailed standard operation procedures or revise the existing regulations according to the business characteristics.

Article 99. Periodic Review of the Guideline

The Guideline shall be reviewed at least once annually in order to reflect the latest development status of the personal information protection-related laws, technologies and businesses, as well as to ensure the effectiveness of personal information security maintenance operation.

Article 100. Planning and Drilling Emergency Responses for Personal Information Incidents

The Company and subsidiary shall perform the emergency responsive plan drill operation for personal information infringement incidents at least annually, and shall preserve relevant records for review.

Article 101. Additional Provisions

Any matters not specified in the Guideline shall be handled according to relevant laws of the competent authority and related Company regulations.

Article 102. Implementation and Revision

The Guideline shall be approved by the Company's president and announced and implemented based on the Company's policy on establishing rules and regulations. The same is true for revisions.

Table: Record of Changes

| Version | Date of Approval | Effective Date | Approval Level | Note: |
|---------|------------------|----------------|----------------|-------|
| 01 | 2012/10/04 | -- | President | |
| 02 | 2013/12/03 | -- | President | |
| 03 | 2014/03/31 | -- | President | |
| 04 | 2015/09/10 | -- | President | |
| 05 | 2016/04/18 | -- | President | |
| 06 | 2017/04/06 | -- | President | |
| 07 | 2019/05/19 | 2019/05/27 | President | |

| | | | | |
|----|------------|------------|----------------------------------|--|
| 08 | 2019/10/23 | 2019/10/31 | Head of Risk Management Division | This revision did not involve substantive changes, and it was therefore approved by the division-level head of the unit responsible for the Policy in accordance with the Company's policy on establishing rules and guidelines. |
| 09 | 2020/07/22 | 2020/07/30 | Head of Risk Management Division | This revision did not involve substantive changes, and it was therefore approved by the division-level head of the unit responsible for the Policy in accordance with the Company's policy on establishing rules and guidelines. |
| 10 | 2022/03/10 | 2022/03/18 | President | |
| 11 | 2023/04/13 | 2023/04/14 | Head of Risk Management Division | Amendment on format and wording pursuant to "The Policy for the formulation of the Internal Rules and Regulations" of the Company that did not involve any change of substance. |
| 12 | 2024/11/05 | 2024/11/20 | President | |
| 13 | 2024/12/03 | 2024/12/03 | Head of Risk Management Division | Amendment on format and wording pursuant to "The Policy for the formulation of the Internal Rules and Regulations" of the Company that did not involve any change of substance. |

附件一

| | |
|--------------------|--|
| 個人資料侵害事故通報表 | |
|--------------------|--|

| | |
|---------------|--|
| 事件發生時間 | |
|---------------|--|

| | | |
|-------------------------|--|--|
| 事件發生種類 | <input type="checkbox"/> 竊取 <input type="checkbox"/> 洩漏 <input type="checkbox"/> 竄改 <input type="checkbox"/> 毀損 <input type="checkbox"/> 滅失 <input type="checkbox"/> 其他侵害 事故 | 個資侵害之總筆數 (大約) _____ |
| | | <input type="checkbox"/> 一般個資 _____ 筆 <input type="checkbox"/> 特種個資 _____ 筆 |
| 發生原因及事件摘要 | | |
| 損害狀況 | | |
| 個資外洩可能結果 | | |
| 擬採取之因應措施 | | |
| 擬採通知當事人之時間及方式 | | |
| 是否於發現個資外洩當日通報作業風險暨綜合規劃部 | <input type="checkbox"/> 是 <input type="checkbox"/> 否，理由 | |

註1：各欄位資訊若尚未明確，得先填寫「不明」，並俟明確後再通報更新補充。

事件發生單位或權責單位：

主管：

覆核：

經辦：

金控風險控管處簽收： 年 月 日 時 分

金控稽核處簽收： 年 月 日 時 分

Attachment 1

| | |
|---|--|
| Personal Information Infringement Incident Reporting Form | |
| Time Incident Occurred | |

| | | |
|--|---|--|
| Type of Incident | <input type="checkbox"/> Theft <input type="checkbox"/> Leak <input type="checkbox"/> Alteration <input type="checkbox"/> Damage <input type="checkbox"/> Loss <input type="checkbox"/> Other breach | Total number of personal information breaches (roughly) _____ |
| | | <input type="checkbox"/> No. of regular personal information breaches _____ <input type="checkbox"/> No. of special personal information breaches _____ |
| Cause of incident and incident summary | | |
| Damage incurred | | |
| Potential result of personal information leak | | |
| Planned response measures | | |
| Planned time/method for notifying data subjects | | |
| Was Operational Risk & Planning Department notified of personal information leak on day it was discovered? | <input type="checkbox"/> Yes <input type="checkbox"/> No, reason why not: | |

Note 1: If information for any of the questions is not clear, please write “unclear”; once clear information is available, please provide an updated version of the form.

Unit in which incident occurred or responsible unit:

Manager:

Reviewed by:

Processed by:

Signed by Fubon Financial Holdings Risk Management Division: (Y/M/D & time) _____

Signed by Fubon Financial Holdings Audit Division: (Y/M/D & time) _____

附件二

| |
|----------------|
| 個人資料侵害事故通報與紀錄表 |
|----------------|

| | | | |
|--|--|--|---|
| 非公務機關名稱 _____ 通報機關 _____ | 通報時間： 年 月 日 時 分 通報人： 簽名(蓋章) 職稱： 電話： Email： 地址： | | |
| 事件發生時間 | | | |
| 事件發生種類 | <table border="1"> <tr> <td> <input type="checkbox"/>竊取 <input type="checkbox"/>洩漏 <input type="checkbox"/>竄改 <input type="checkbox"/>毀損 <input type="checkbox"/>滅失 <input type="checkbox"/>其他侵害 事故 </td> <td> 個資侵害之總筆數 (大約) _____ <input type="checkbox"/>一般個資 _____ 筆 <input type="checkbox"/>特種個資 _____ 筆 </td> </tr> </table> | <input type="checkbox"/> 竊取 <input type="checkbox"/> 洩漏 <input type="checkbox"/> 竄改 <input type="checkbox"/> 毀損 <input type="checkbox"/> 滅失 <input type="checkbox"/> 其他侵害 事故 | 個資侵害之總筆數 (大約) _____ <input type="checkbox"/> 一般個資 _____ 筆 <input type="checkbox"/> 特種個資 _____ 筆 |
| <input type="checkbox"/> 竊取 <input type="checkbox"/> 洩漏 <input type="checkbox"/> 竄改 <input type="checkbox"/> 毀損 <input type="checkbox"/> 滅失 <input type="checkbox"/> 其他侵害 事故 | 個資侵害之總筆數 (大約) _____ <input type="checkbox"/> 一般個資 _____ 筆 <input type="checkbox"/> 特種個資 _____ 筆 | | |
| 發生原因及事件摘要 | | | |
| 損害狀況 | | | |
| 個資外洩可能結果 | | | |
| 擬採取之因應措 | | | |
| 擬採通知當事人之時間及方式 | | | |
| 是否於發現個資外洩後72小時通報金管會 | <input type="checkbox"/> 是 <input type="checkbox"/> 否，理由 | | |

註1：各欄位資訊若尚未明確，得先填寫「不明」，並俟明確後再通報更新補充。

註2：上開72小時通報金管會，例假日均納入時效計算。

Attachment 2

| Personal Information Infringement Incident Reporting and Recording Form | | |
|--|---|--|
| Non-government Agency Name _____ Agency Notified _____ | Time reported (Date/time): Reporting person: _____ Signature (chop) Position: Phone: Email: Address: | |
| Time Incident Occurred | | |
| Type of Incident | <input type="checkbox"/> Theft <input type="checkbox"/> Leak <input type="checkbox"/> Alteration <input type="checkbox"/> Damage <input type="checkbox"/> Loss <input type="checkbox"/> Other Breach | Total number of personal information breaches (roughly) _____ <input type="checkbox"/> No. of regular personal information breaches _____ <input type="checkbox"/> No. of special personal information breaches _____ |
| Cause of incident and incident summary | | |
| Damage incurred | | |
| Potential result of personal information leak | | |
| Planned response measures | | |
| Planned time/method for notifying data subjects | | |
| Was FSC notified of personal information leak within 72 hours of when it was discovered? | <input type="checkbox"/> Yes <input type="checkbox"/> No, and reason why not: | |

Note 1: If information for any of the questions is not clear, please write “unclear”; once clear information is available, please provide an updated version of the form.

Note 2: Regular holidays are included in the 72-hour deadline for notifying the FSC of a personal information leak.