Chang Hwa Commercial Bank Personal Information File Security Management Program

Formulated by board of directors' meeting on June 30, 2014
Amendment approved by board of directors' meeting on December 23, 2016
Amendment approved by board of directors' meeting on January 23, 2019
Amendment approved by board of directors' meeting on January 24, 2022

Article 1

In order to fulfill personal information file security management, pursuant to Article 3 of the Regulation Governing Non-Government Agency Personal Information Data Security Protection Designated by Financial Supervisory Commission, R.O.C.(Taiwan), Chang Hwa Commercial Bank Ltd. (the "Bank") does hereby promulgate the Personal Information File Security Management Program (the "Program").

Article 2

The Program is applied to personal information be collected, proceeded and used by all business processing.

Article 3

For purposes of the Program only, the following definitions shall apply:

(a) E-commerce means advertisement, marketing, supply, order or delivery of merchandise or service via internet.

(b) Media means such as papers, magnetic disks, magnetic tapes, optical disks, microfilms, integrated circuits, computers, automated machines or other those personal data are stored on or in.

(c) Significant Personal Information Security Incident means the situation that personal information being stolen, altered, damaged, destroyed or disclosed endanger the Bank's regular operation or imperil enormous party's rights and interests.

(d) Log Files means derive information (include but not limit to log trail, party's account, access time, device ID and Internet protocol (IP) address) whenever personal information be collected, proceeded and used.

Article 4

All units should deploy personal information protection personnel and enough resources to draw up and carry out the Program.

Article 5

The Bank should, in line with applicable personal information protection laws and regulations,

periodically review status of all personal information collected and define the scope of the Program .

Article 6

The Bank should assess the risk raised from the collecting, processing and using of personal information and establish adequate personal information management mechanism based on the risk assessment's result.

Article 7

The Bank should establish internal management procedures about personal information collecting, processing and using, the below should be included:

(a) Reviewing the specific purpose and regulatory compliance for collecting, processing and using the sensitive personal information defined by Article 6 of the Personal Information Protection Act (the "Law") are in accordance with the regulation's needs. Make sure while collecting, processing and using the sensitive personal information by written consent of party are in accordance with Paragraph 1, 2 and 4 of Article 7 apply mutatis mutandis to Paragraph 2 Article 6 of the Law.

(b) Unless specified otherwise in the Law, collecting personal information need to fulfill the obligation of disclosure and make sure the content and method are legitimate and adequate.

(c) Reviewing non-sensitive personal information collection and processing has a specific purpose and should comply with conditions of Article 19 of the Law; Ensure collecting and processing under consent given by the party should be in according with Article 7 of the Law.

(d) Ensuring the using of non-sensitive personal information is in accordance with the scope of the specific purpose of collection provided by Article 20 of the Law. The non-sensitive personal information may be used outside the scope upon the occurrence of one of the conditions provided by Article 20 of the Law; ensuring the using is under consent given by the party should be in according with Article 7 of the Law.

(e) When using the personal information for the purpose of marketing and has been turned down by the party, the Bank should immediately cease using the party's personal information for marketing.; the charge-free approach of refusal shall be provided to the party at the first marketing action.

(f) When commissioning third party to collect, process or use personal information, the Bank shall properly supervise the third party in accordance to Article 8 of Enforcement Rules of the Personal Information Protection Act and expressly arrange the content in the contract or related document.

(g) Before cross-border processing or using personal information, review if the international transmission is in the restrict scope arranged by the Financial Supervisory Commission, R.O.C.(Taiwan).

(h)the following items about rights of Article 3 of the Law exercised by party with regard to his/her personal information:
   1. Identifying the party.
   2. Providing the approach to exercise the rights of party, inform the expense needed, and items need to be clarified.
   3. The approach of reviewing the party's request, and comply with the deadline prescribed by the Law.
   4. The reason according to the Law may be applied to refuse of exercise rights of party, the approach of recording the reason of refusal and notifying the party.

(i) Check the accuracy of personal information's while collecting, processing or using; In the event of inaccuracy or a dispute regarding the accuracy of personal information, the procedures should be adopted according to Paragraph 1, 2 and 5 of the Article 11 of the Law.

(j) Check if the specific purpose of keeping the personal information is no longer exists or upon expiration of the relevant time period; the information collected should be deleted, discontinued to process or use according to Paragraph 3 of the Article 11 of the Law when the purpose of keeping the personal information is no longer exists or upon expiration of the relevant time period.

Article 8

For the personal information security purpose, the Bank should establish personal information security management approaches for the followings:

(a) E-commerce service system information security approaches:
   1. User's authentication assurance and protection mechanism.
   2. Personal information display masking mechanism.
   3. Internet transit secure encryption mechanism.
   4. Software verification and validation procedures of Application's development, go-live and maintenance stages.
   5. Personal information file and database access control and protective monitor approach.
   6. Strategies of preventing external network invasion.
   7. Monitoring and response mechanism of illegal or unordinary use.
   8. Periodical testing, reviewing and improving for Item 6 and 7 of this Subparagraph.

(b)Establish using guideline for each equipment and storage media, and adopt adequate approach for preventing data breach when scrapping or reassigning the equipment and storage media.

(c) Adopt adequate encrypting approach for the personal information needed encryption when collecting, processing and using.

(d)Adopt adequate protection for backup personal information when process has the backup needs.

(e) Adopt equipment safety management approaches for media those who storage personal

information.

1. Implement adequate access control.
2. Set up adequate custody for media.
3. Build up adequate protecting equipment or technic according to the characteristics of media and its environment.

(f) According to the necessity of executing business, establish the clearance of relevant personnel to access personal information and control their access situation, and an agreement with personnel designed to confidential obligation.

Article 9

In order to prevent personal information from being stolen, altered, damaged, destroyed or leaked, the following response, notification and prevention mechanisms should be adopted:

(a) Post-incident related response activities including:

1. Approaches about controlling damages of the Party.
2. Adequate approaches about notifying the Party after an inspection of the incident.
3. Contents about fact of incident should be notified, response has been taken and consulting service line.

(b) The person those whose notice is required to be provided to and the approach of notification.

(c) The communication-panel-mechanism for post-incident corrective and preventive approaches.

In the event of a serious personal information data breach incident, the Financial Supervisory Commission, R.O.C.(Taiwan) should be notified within 72 hours. However, when other regulations provide otherwise, it shall be carried out in accordance with the regulations. The corrective and preventive approaches in the third subparagraph of preceding paragraph should be subject to an overall diagnosis and examination by an expert who is impartial, independent and has obtained relevant recognized accreditation qualifications.

Article 10

The Bank should provide personal information protection awareness propaganda and training for all employees periodically to make them all understood the requirement of relevant regulations, scope of responsibilities and various personal information protection mechanisms, procedures and approaches.

Article 11

All personal information protection mechanisms, procedures and approaches implemented in accordance with the Program should be contained within internal audit and self-exam function.

Article 12

The Bank executes all personal information protection mechanisms, procedures and approaches

implemented in accordance with the Program should record the using of personal information and maintain the data trail or relevant evidence.

Article 13

Unless specified otherwise in regulations, while the specific purpose of collecting personal information no longer exists or the time period expires, the personal information shall be deleted, discontinued to process or use and keep the below record for reference.

(a) The approach and time of deleting, discontinuing to process or using.

(b) When the deleting, discontinuing to process or using of personal information be transferred to a third party, the reason, the party, method and time of the transfer, and the legitimacy of the third party.

Except as otherwise provided in regulations or in contracts, the tracking information, related document and record of preceding Article and preceding Paragraph should be maintained for a period of five years.

Article 14

To consistently improve the Bank's personal information security process, related business divisions should provide the self-assessment report for their execution annually.

The abovementioned report should be summarized and submitted to Execute Board of Directors for review after getting General Manager's approval.

The self-assessment report should include the processing of planning, implementation of improvement and adoption of preventive approach for concern of regulation's breach matter.

Article 15

General Manager is authorized to approve the personal information protection mechanism, procedures and enforcement rules prescribed by this Program; related business divisions shall review it periodically and revise it if necessary.

When the Bank's Head Office need to set out other relevant mechanisms, procedures and measures in order to comply with the personal information protection regulations of the host locations of its overseas branches, the preceding paragraph may be applicable.

Article 16

The Program shall be implemented after approved by Board of Directors, and the same shall apply for modification.