

# Shanghai Commercial and Savings Bank Personal Information Management Policy

Instituted under strategic planning of the General Administration Division

Instituted on 2015.11.21

## Article I: Purpose

The Personal Information Management Policy (hereinafter referred to as “This Policy”) is instituted in compliance with the Personal Information Protection Act (hereinafter referred to as “PIPA”) and other applicable legal rules governing the protection of personal information for fortifying the management, protection, and execution of personal information of the Bank.

## Article II: Scope

This Policy is the fundamental framework for the protection of personal information at the Bank and shall be duly observed by all of the employees.

## Article III: Terms and definitions

Personal information as referred to in This Policy shall be defined by PIPA and other applicable legal rules governing the protection of personal information.

## Article IV: Competent Authority

The Bank has established the “Personal Information Protection Management Team” for the routine review of the pursuit of personal information protection in conformity to the requirements of PIPA and other applicable legal rules. The regulations governing the establishment of the “Personal Information Protection Management Team” shall be subject to the approval of the General Manager through empowerment and announcement for causing into full force. The same procedure is applicable to any amendment thereto.

## Article V: Legitimate collection, processing, and use

The Bank shall collect, process, and use personal information for the authorized business under the operation of legitimate organization through reasonable and secure means within designated scope.

#### Article VI: The accuracy of personal information

The Bank shall create and maintain files containing personal information, and proceed to update where necessary for assurance of the accuracy of personal information.

#### Article VII: Management of the risk inherent to personal information

The Bank shall set the standard for determination of the level of risk inherent to the files containing personal information in order to manage the risks inherent to the files containing personal information at a tolerable threshold, and set the retention period for related documents in conformity to the requirements of PIPA and other applicable legal rules.

#### Article VIII: Security policy for the protection of personal information

The Bank shall establish and design relevant measures for personal information protection management for assurance of the proper implementation of the personal information management system. The Bank shall also protect the personal information collected, processed, and used by the Bank with expected reasonable security management technology.

#### Article IX: Reasonable allocation of resources

The Bank shall consider the reasonable allocation of corporate resources through proper staffing of managerial personnel and appropriate level of resources for the design, establishment, revision, and implementation of the personal information file security protection plan.

#### Article X: Personal information liaison window

All banking units of the Bank shall establish windows for the liaison and management of personal information charged with the duties of the implementation of the personal information protection management system and the availability of the exercise of the rights of the parties concerned regarding personal information and related inquiries.

#### Article XI: Personal Information Security Incidents

The Bank shall institute rules and regulations governing the notification of personal information security incidents to regulate the notification of the occurrence of security information incident, responses to the theft, modification, damage, missing, or divulgence of personal information and other material incidents.

#### Article XII: The management and supervision of outsourced services for

personal information

The Bank may outsource third-party service providers to collect, process, and use personal information, and shall supervise the outsourced contractors in due diligence thereby explicitly set forth the responsibility of information security and the obligation of confidentiality. Such requirements shall be inscribed as an integral part of the outsourced agreement binding the outsourced contractors. The Bank shall conduct routine audits on the operation.

#### Article XIII: Protection of personal information transmission

The Bank shall establish transmission mechanisms capable of proper transmission for assurance of the security of transmitting personal information in domestic and overseas.

#### Article XIV: Routine Evaluation

The Bank shall run the personal information protection system on a perpetual basis for assurance of the security of personal information files, and present related reports at regular intervals.

#### Article XV: Miscellaneous

Anything not mentioned in This Policy shall be governed by other applicable legal rules or the internal rules and regulations of the Bank.

#### Article XVI

This Policy shall come into force at the final approval of the Board. The same procedure is applicable to any amendment thereto.