南京银行数据安全与客户信息保护管理政策要点

Key Points of Data Security and Customer Information Protection Management Policy of Bank of Nanjing

南京银行股份有限公司（简称“本行”）高度重视数据安全保护，建立覆盖数据全生命周期的数据安全保护机制。根据《中华人民共和国网络安全法》《中华人民共和国消费者权益保护法》《中华人民共和国个人信息保护法》《中国人民银行金融消费者权益保护实施办法》等外部法律法规，以及《南京银行数据管理办法》等内部制度管理要求，制定《南京银行数据安全管理办法》和《南京银行客户个人金融信息保护工作管理办法》，夯实数据安全责任制，配套制定全生命周期、事件应急等基础管理类规范，同步发布数据对外提供、信息系统等重点专项类规范，防控重点领域数据安全风险，切实筑牢数据安全底线。

Bank of Nanjing Co., Ltd. (“the Bank”) attaches great importance to data security and has established a data protection mechanism covering the data life cycle. Based on laws and regulations such as the *Data Security Law of the People’s Republic of China*, the *Law of the People’s Republic of China on the Protection of Consumer Rights and Interests*, the *Personal Information Protection Law of the People’s Republic of China*, the *Implementation Measures of the People’s Bank of China for*

the Protection of Financial Consumer Rights, as well as the Bank's management policies including the *Measures for Data Management of Bank of Nanjing*, the Bank developed the *Measures for Data Security Management of Bank of Nanjing* and the *Administrative Measures for the Protection of Customers' Personal Financial Information of Bank of Nanjing* to implement the accountability system for data security, and issued supporting basic management standards covering full data life cycle and incident emergency response, as well as special rules on cross-border data transfers and information systems, to prevent and contain data security risks in key areas, safeguarding the bottom line of data security.

一、适用范围

I. Scope of Application

数据安全管理范围覆盖境内各级机构全部业务线。

The data security management covers all business lines of domestic entities at all levels.

《南京银行数据安全管理办法》《南京银行客户个人金融信息保护工作管理办法》适用于本行各级分支机构和总行各部室。

The *Measures for Data Security Management of Bank of Nanjing* and the *Administrative Measures for the Protection of Customers' Personal Financial Information of Bank of Nanjing* are applicable to Bank's all branches and all departments at the

Head Office.

二、总体原则

II. General Principles

1．本行数据安全管理遵循以下策略和原则：

1. The Bank’s data security management adheres to the following strategies and principles:

（1）协同发展。构建总行统筹协调、业务条线执行、内控防线监督的三维联动机制，深化业务与技术的融合创新。将数据风险控制纳入常态化管理流程，形成全员参与、分层负责的安全治理体系，推动防护责任向基层穿透式传导。

(1) Synergistic development. Establish a three-dimensional collaboration mechanism where the Head Office provides overall coordination, business lines execute operations, and internal control functions supervise implementation. Deepen integrated innovation between business and technology by incorporating data risk control into routine management processes. Establish a security governance system featuring full participation and tiered accountability, promoting the vertical penetration of protection responsibilities to the execution level.

（2）科技赋能。推行人防与技术防护协同的立体防护体系，重点部署智能化数据管控技术，建立全流程加密传输与权限隔离机制，推动数据安全领域技术创新应用，实施数据全流程管控。

(2) Technology enablement. Implement a multi-

dimensional protection system that combines human defense with technical safeguards, prioritizing the deployment of intelligent data management technologies. Establish end-to-end encryption transmission and permission isolation mechanisms, promote innovative technology applications in data security, and implement full-lifecycle data control.

（3）动态平衡。注重数据安全防护与价值释放的协同发展，严格遵循相关法律法规和标准规范实施安全防护，为数据要素的高效流通与深度赋能提供保障。

(3) Dynamic balance. Strike a harmonized balance between data security protection and value realization. Strictly adhere to relevant laws and regulations as well as industry standards while establishing a robust framework to enable efficient data circulation and comprehensive application.

2．本行客户信息保护遵循以下策略和原则：

2. The Bank’s customer information protection adheres to the following strategies and principles:

（1）本行遵循目的明确、公开透明、安全保障、知情同意、责任落实等基本原则，依法处理客户个人金融信息。

(1) The Bank adheres to core principles including purpose specification, transparency, data security, informed consent, and accountability in processing personal financial information, ensuring compliance with applicable laws.

（2）本行收集个人金融信息时，遵循合法、合理、必要

原则，经客户明示同意。不得收集与业务无关的客户个人金融信息，不得采取不正当方式收集，不得变相强制收集，不得以客户不同意处理其个人金融信息为由拒绝提供金融产品及服务，但处理其个人金融信息属于提供金融产品及服务所必需的除外。

(2) When collecting personal financial information, the Bank ensures lawful, legitimate, and necessary collection practices with explicit customer consent. Prohibited practices include collecting information unrelated to business operations; using improper methods for collection; implementing covert coercion; or denying financial products/services solely based on customer refusal to provide personal financial information, except when processing such information is indispensable for providing financial products/services.

三、管理架构

III. Management Structure

（一） 董事会

(I) Board of Directors

本行董事会承担信息科技风险管理最终职责，负责披露信息科技风险管理制度和流程，确保信息科技风险能够被识别、评估、计量、监测和控制。同时，董事会作为数据安全管理的决策机构，负责制定数据战略，审批或授权审批与数据管理相关的重大事项，对本行数据安全工作负主体责任。

The Board of Directors bears ultimate responsibility for IT risk management, responsible for disclosing the management policies and processes for IT risk, ensuring that IT risks are identified, assessed, measured, monitored, and controlled. Additionally, as the decision-making body for data security management, the Board formulates data strategies, provides or authorizes the approval for material matters related to data governance, and bears primary accountability for the Bank's data security initiatives.

本行董事会可授权风险管理委员会履行信息科技风险管理的部分职责，包括听取高级管理层信息科技风险监测报告等。

The Board of Directors may delegate to the Risk Management Committee the authority to assume certain responsibilities for IT risk management, including such duties as reviewing IT risk monitoring reports submitted by senior management.

本行董事会下设消费者权益保护委员会，负责指导并督促高级管理层有效执行和落实消费者权益保护中消费者金融信息保护相关工作，并定期听取高级管理层工作开展情况报告。

The Board of Directors has established a Consumer Rights and Interests Protection Committee, responsible for guiding and supervising senior management to effectively implement

consumer financial information protection initiatives within the broader framework of consumer rights and interests protection, and regularly reviewing progress reports submitted by senior management.

（二） 高级管理层

(II) Senior management

本行设置信息科技管理委员会，由行长担任主任，首席信息官担任副主任，委员会负责统筹监督信息科技管理各项工作，并定期向董事会和高级管理层汇报整体运行情况。

The Bank has established an Information Technology Management Committee, chaired by the President and vice-chaired by the Chief Information Officer. The Committee responsible for overseeing overall IT management operations and regularly reporting comprehensive operational status to both the Board of Directors and senior management.

本行成立数据管理委员会，负责本行数据安全相关事项的审议决策、组织部署和指导监督，听取数据安全工作整体情况汇报。

The Bank has established a Data Management Committee responsible for decision-making, coordination and supervision on data security-related matters, and regularly reviewing comprehensive reports on data security operations.

（三） 各分行、总行各部室

(III) Branches and Head Office departments

各分行、总行各部室按照“谁管业务、谁管业务数据、谁管数据安全”的原则，负责本条线数据安全管理工作，组织落实数据安全管理要求。总行信息技术部、数字银行管理部是数据安全的技术保护部门；总行法律合规部负责将数据安全纳入全行合规管理体系，指导、督促数据安全牵头管理部门开展数据检查、问题整改以及问责相关工作；总行审计部负责定期对全行数据安全的管理状况进行审计。专项领域牵头部门负责在其专项领域推动落实数据安全管理要求，持续强化数据安全集团一体化管理。

Each branch/Head Office department is responsible for data security management within their respective business lines, organizing the implementation of data security management requirements according to the principle of “Whoever manages the business, manages the business data and assumes responsibility for data security”. The Head Office Information Technology Department and Digital Banking Management Department are responsible for technical protection for data security; the Head Office Legal and Compliance Department integrates data security into the bank-wide compliance management framework, guiding and supervising data security lead departments to conduct data security audits, implement corrective actions, and manage accountability-related work; the Head Office Audit Department

conducts regular audits of the Bank's data security management status. Lead departments for specific domains are responsible for driving the implementation of data security management requirements within their specialized areas. The Bank continuously strengthens integrated bank-wide data security governance.

四、关键定义

IV. Key Definitions

客户个人金融信息

Customer's Personal Financial Information

客户个人金融信息，是指本行通过开展业务或者其他合法渠道处理的消费者信息。消费者信息的处理包括消费者信息的收集、存储、使用、加工、传输、提供、公开等。

Customer's personal financial information refers to consumer information processed by the Bank during business operations or through other lawful channels. Processing of consumer information includes information collection, storage, use, processing, transmission, provision, disclosure, and other activities.

客户个人金融信息包括以下个人信息：

Customer's personal financial information includes the following personal data:

1．个人身份信息，包括个人姓名、性别、国籍、民族、身份证件种类号码及有效期限、职业、联系方式、婚姻状况、

家庭状况、住所或工作单位地址及照片等；

1. Personal identity information, including name, gender, nationality, ethnicity, type, number and validity period of identity documents, occupation, contact details, marital status, family status, residential or workplace address, and photographs;

2．个人财产信息，包括个人收入状况、拥有的不动产状况、拥有的车辆状况、纳税额、公积金缴存金额等；

2. Personal property information, including income, ownership of real estate, ownership of vehicles, tax amounts, and housing fund contributions;

3．个人账户信息，包括账号、账户开立时间、开户行、账户余额、账户交易情况等；

3. Personal account information, including account numbers, account opening date, opening branch, account balance, and transaction history;

4．个人信用信息，包括信用卡还款情况、贷款偿还情况，以及个人在经济活动中形成的、能够反映其信用状况的其他信息；

4. Personal credit information, including credit card repayment records, loan repayment status, and other information that reflects an individual’s creditworthiness formed in economic activities;

5．个人金融交易信息，包括本行在支付结算、理财、保险箱等中间业务过程中获取、保存、留存的个人信息和客户

在通过本行与保险公司、证券公司、基金公司、期货公司等第三方机构发生业务关系时产生的个人信息等；

5. Personal financial transaction information, including personal data obtained, stored, or retained during fee-based services such as payment settlements, wealth management, and safe deposit box operations, as well as information from the customer's transactions with third-party institutions (e.g., insurance companies, securities firms, fund management companies, futures companies) through the Bank;

6．衍生信息，包括个人消费习惯、投资意愿等对原始信息进行处理、分析所形成的、反映特定个人某些情况的信息；

6. Derived information, including consumption habits, investment preferences, and other information that reflects specific personal characteristics, derived from analysis or processing of original data;

7．在与个人建立业务关系过程中获取、保存的其他个人信息。

7. Other personal information obtained or retained during the establishment and maintenance of business relationships with the individual.

五、客户信息的收集

V. Collection of Customer Information

本行遵循目的明确、公开透明、安全保障、知情同意、责任落实等基本原则，依法处理客户个人金融信息。

The Bank adheres to core principles including purpose specification, transparency, data security, informed consent, and accountability in processing personal financial information, ensuring compliance with applicable laws.

1．本行收集个人金融信息时，遵循合法、合理、必要原则，经客户明示同意。不得收集与业务无关的客户个人金融信息，不得采取不正当方式收集，不得变相强制收集，不得以客户不同意处理其个人金融信息为由拒绝提供金融产品及服务，但处理其个人金融信息属于提供金融产品及服务所必需的除外。

1. When collecting personal financial information, the Bank ensures lawful, legitimate, and necessary collection practices with explicit customer consent. Prohibited practices include collecting information unrelated to business operations; using improper methods for collection; implementing covert coercion; or denying financial products/services solely based on customer refusal to provide personal financial information, except when processing such information is indispensable for providing financial products/services.

2．本行按最小必要原则采集客户个人信息，未经客户同意，不从第三方收集个人数据（法律要求的情况除外）。本行收集消费者的个人信息的方式包括：

2. The Bank shall collect personal information under the minimum necessity principle and shall not obtain personal data

from third parties without the customer's consent, except where required by law. Methods for collecting personal information include:

（1）向消费者提供服务时其主动提供的个人信息；

(1) Personal information provided by the customer during the provision of services.

（2）向消费者提供金融服务过程中形成的与服务相关的信息；

(2) Data generated during the provision of financial services that is related to such services.

（3）按照法律、行政法规，向征信机构、信用管理公司、资信评估机构等合法留存个人信息的自然人、法人以及其他组织收集为消费者提供服务所必要的个人信息；

(3) Required personal information collected from lawful entities (e.g., credit reference agencies, credit management companies, credit rating agencies) in compliance with laws and administrative regulations to deliver services.

（4）法律法规规定或经消费者许可的其他方式。

(4) Other methods as stipulated by laws and regulations or permitted by the customer.

六、客户信息的使用

VI. Use of Customer Information

本行按照法律法规的规定和双方约定的用途正确使用客户个人金融信息，不得超出范围使用。

The Bank properly uses customers' personal financial information in accordance with applicable laws, regulations, and agreed-upon purposes, without exceeding the prescribed scope.

1. 本行通过界面展示客户个人金融信息的，除实现业务目的所必需外，应对需要展示的个人金融信息采取去标识化处理等措施，降低个人金融信息在展示环节的泄露风险。

1. When displaying customers' personal financial information through interfaces, the Bank shall, except for what is strictly necessary to achieve business purposes, apply measures such as de-identification to the personal financial information to be displayed, thereby minimizing the risk of breach during the display process.

2. 本行加工目的应与采集时的约定一致，不以垄断经营和不正当竞争为目的，不发生误导、欺诈、胁迫或者干扰等限制个人或者组织正当选择与决策的行为，遵循社会公德伦理。

2. The Bank's processing purposes shall be consistent with those agreed upon at the time of data collection. It shall not use the information for monopolistic practices or unfair competition, nor engage in behaviors such as misguidance, fraud, coercion, or interference that restrict individuals' or organizations' legitimate choices and decision-making. The Bank shall adhere to societal ethics and moral standards.

3. 本行因工作需要调阅个人金融信息档案资料或电子

数据时严格履行审批手续，并留存审批和调阅记录，以备追溯；采取有效技术措施，确保信息在内部使用及对外提供等流转环节的安全和可追溯，防范信息泄露风险。

3. When the Bank needs to access personal financial information records or electronic data for work purposes, it strictly follows approval procedures, retains records of approval and access for traceability, and implements effective technical measures to ensure the security and traceability of information throughout internal use and external sharing processes, thereby preventing risks of data breach.

4. 加强柜面个人金融信息查询管理，规范查询本人、代理查询他人账户存款等个人金融信息的程序，审核对方有效身份证件或有关法律文书，防止个人金融信息泄露。

4. The Bank strengthens the management of in-branch inquiries into personal financial information, standardizes procedures for querying account deposits, whether for oneself or on behalf of others, and verifies the valid identification documents of the inquirer or relevant legal documentation to prevent the breach of personal financial data.

5. 本行员工严格遵守法律法规和监管要求，依法使用工作中获取的客户信息，不得以任何形式进行以下行为:

5. Bank employees strictly comply with laws, regulations, and supervisory requirements, and use customer information obtained in work in compliance with laws, and shall not engage

in the following acts in any form:

（1）出售客户信息。

(1) Sell customer information.

（2）向行内无关人员或行外人员泄露客户信息。

(2) Disclose customer information to unrelated people within or outside the Bank.

（3）违规收集、加工、使用、存储或向第三方提供本行客户信息及内部数据，损害本行或客户合法权益。

(3) Illegally collect, process, use, retain, or provide the Bank's customer information or internal data to third parties, thereby harming the Bank's or customers' legitimate rights and interests.

（4）利用职务便利擅自截留、修改、骗取客户信息。

(4) Abuse job authority to unlawfully retain, tamper, or fraudulently obtain customer information.

（5）未经消费者授权或同意向第三方提供消费者个人信息（法律、法规等另有规定的除外）。

(5) Provide consumers' personal information to third parties without their authorization or consent (except where otherwise stipulated by law, regulations, or other provisions).

（6）其他违法使用客户信息的行为。

(6) Other illegal uses of customer information.

七、客户信息的存储

VII. Retention of Customer Information

1. 本行严格执行档案管理和电子数据管理相关规定，采取技术措施和其他必要措施，妥善保管和存储所收集的个人金融信息，防止信息遗失、毁损、泄露或者篡改。在发生或者可能发生个人金融信息遗失、毁损、泄露或者篡改等情况时，应当采取适当的方式告知客户。

1. The Bank strictly adheres to regulations on archival management and electronic data management regulations, employing technical and other necessary measures to properly safeguard and retain collected personal financial information, preventing loss, damage, breach, or tampering. In the event of or where there is a possibility of leakage, damage, loss or tampering of customer information, the Bank shall promptly inform affected customers through appropriate means.

2. 对于互联网应用系统，个人身份鉴别数据应使用密码算法进行字段级加密存储。

2. For internet-based application systems, personal identity authentication data shall be encrypted at the field level using cryptographic algorithms.

3. 本行应按照国家、行业有关规定及与数据主体的约定进行数据删除或匿名化处理。本行委托数据处理中止时应要求服务提供商及时删除数据，确保数据被销毁、不可恢复。

3. The Bank shall delete or anonymize data in accordance

with national and industry regulations, as well as agreements with data subjects. Upon termination of data processing services, the Bank shall require service providers to promptly delete data and ensure that the data are permanently destroyed and cannot be recovered.

八、客户信息的保护

VIII. Protection of Customer Information

（一） 制度与风险管理体系建设

(I) Development of rules and risk management system

客户个人金融信息纳入本行数据安全等级管理，按照《信息安全技术个人信息安全规范》区分一般个人金融信息和敏感个人金融信息，实行分类区别保护。针对敏感个人金融信息，应按照本行数据分级及使用权限管理要求，采取更严格的管理措施。

Customers' personal financial information falls under the Bank's data security classification management framework. It is categorized into general personal financial information and sensitive personal financial information in accordance with the *Information Security Technology - Personal Information Security Specification*, for which classified protection measures shall be taken. For sensitive personal financial information, the Bank shall take stricter management measures in compliance with the Bank's requirements for data grading and access management.

（二） 数据安全技术与管理措施

(II) Data security technology and management measures

1. 本行加强涉及个人信息的岗位权限管理，确保其权限与职责相匹配，防止不相关部门、岗位和人员未经授权查询、泄露、损毁与篡改个人信息。

1. The Bank shall intensify the management of position-specific access involving personal information, to ensure that individuals' access is aligned with their job duties, and to prevent unrelated departments, roles or personnel from unauthorized query, revelation, destruction, or tampering of personal information.

2. 本行切实落实项目建设中对客户数据信息的访问控制。

2. The Bank shall effectively implement access control over customer data information during project development.

（1）明确依照规范执行数据的下载、使用、保存、传输、销毁以及非计划性修改等操作流程。

(1) Clarify operating procedures for data download, usage, storage, transmission, destruction, and unplanned modification in accordance with regulatory standards.

（2）加强信息加工环节的管理控制。

(2) Strengthen management and control over information processing.

（3）严格执行外包人员驻场审批报备制度。

(3) Enforce strictly the system of approval and reporting for on-site outsourcing personnel.

（4）建立敏感文件常态化检查机制，通过数据库敏感数据扫描系统和桌面数据防泄密系统，定期扫描全行开发测试环境和办公终端敏感文件，排查潜在安全风险。

(4) Establish the mechanism of routine inspection for sensitive documents, use the database sensitive data scanning system and the desktop data leakage prevention system to conduct regular scans of the Bank's development/test environments and sensitive documents at office terminals, to identify potential security risks.

3. 本行业务系统后台管理或客户经理处理涉及敏感及以上级别数据时，应启用数字水印，批量展示时应脱敏。

3. When back-office management of the Bank's business systems or relationship managers process data classified as sensitive or above, activate digital watermarking, and apply data masking in case of bulk data display.

4. 明确特权账号的使用场景和使用规则，落实安全责任人管理、限制使用地点，使用多因素认证并保留登录及操作日志。

4. Define usage scenarios and operational rules for privileged accounts, implement management of persons in charge of security and restrict access location, enforce multi-factor authentication, and retain login and activity logs.

5. 制定《南京银行数据安全事件应急管理办法》《南京银行数据安全事件应急预案》，明确数据安全事件应急处置原则和处置程序，进一步提升应对数据安全突发事件的应急管理能力。开展数据安全事件应急演练，针对数据泄露、数据滥用、数据篡改、数据窃取等数据安全风险场景，进一步检验应急处置流程和措施的有效性，提升数据安全事件应急处置能力。发生重大及以上数据安全事件后，本行数据安全牵头部门应建立数据安全事件应急管理机制及机构内部协调联动机制，及时处置风险隐患及安全事件。

5. Develop the *Bank of Nanjing Emergency Management Measures for Data Security Incidents* and the *Bank of Nanjing Emergency Response Plan for Data Security Incidents*, which specify principles and procedures for emergency responses to data security incidents, to further enhance capabilities in managing unexpected data security events. Conduct emergency drills for data security incidents, and further validate the effectiveness of emergency response processes and measures under scenarios of data security risks such as data leakage, abuse, tampering, and theft, to strengthen the Bank's capability of emergency response to data security incidents. In the event of a major or higher-level data security incident, the Bank's data security lead department shall establish the emergency management mechanism for data security incidents and the in-

house coordination mechanism to promptly address potential risks and security incidents.

（三） 人员管理与培训

(III) Personnel management and training

1. 本行所有员工应按照《南京银行保密工作管理办法》相关要求在上岗前作出书面保密承诺，签订保密协议，明确保密内容、违约责任及脱密期限等事项。在处理消费者金融信息时，应严格遵守相关法律法规及监管要求，采取有效措施加强对消费者金融信息的保护，确保消费者的金融信息安全。

1. The Bank's employees shall provide written confidentiality commitment and sign confidentiality agreements prior to commencing duties, in accordance with the requirements in the *Bank of Nanjing Confidentiality Management Measures*, to clarify confidential content, breach liability, and declassification period. When processing consumer financial information, the employees shall strictly comply with applicable laws, regulations, and regulatory requirements, and take effective measures to enhance the protection of consumer financial information, to ensure the security of consumer financial information.

2. 加强外包服务人员管理，建立外包服务人员档案制度。对于外包服务人员，应进行必要的宣传、监督与评审，使其知晓在提供外包服务时的信息保护责任。

2. The Bank shall strengthen the management of outsourcing

service personnel by establishing archiving system for outsourcing service personnel. The Bank shall provide necessary promotion, supervision and review for outsourcing service personnel, to ensure they are aware of their information protection responsibilities in the provision of outsourcing services.

3. 将客户个人金融信息保护相关知识培训纳入本机构培训计划，围绕相关法律法规和规章，金融监管部门有关客户个人金融信息保护的相关规定，以及本机构员工行为准则、职业操守等内容，广泛开展教育培训。

3. The Bank shall incorporate training on the protection of customers' personal financial information into the Bank's training program, and provide a wide range of education and training centered on relevant laws, regulations and rules, regulatory provisions of financial regulators for protection of customers' personal financial information, as well as the Bank's employee code of conduct and professional ethics.

4. 本行不断提升数据安全管理队伍建设，坚持将数据安全融入业务管理，在业务条线培训中设置专项数据安全课程，面向全体员工持续开展培训，内容覆盖数据安全法律法规、行内规章制度、重点场景操作流程等，通过录制课程、专题培训、制作短视频、知识测试等方式组织开展。除行内员工外，本行对合作中涉及的服务商和外包人员进行安全教育或培训，同时要求服务商对其服务团队成员进行必要的安

全教育或培训，确保管控措施能够有效落实。

4. The Bank shall continuously improve the construction of its data security management team, pursue the integration of data security into business management, set up special data security courses in business line training, and provide ongoing training to all employees, covering data security laws and regulations, the Bank's internal rules and policies, and operation processes under key scenarios. The training will be organized through various methods such as recorded courses, special training sessions, short videos, and knowledge testing. In addition to internal employees, the Bank shall also provide security education or training for service providers and outsourcing personnel involved in cooperations, and require service providers to conduct necessary security education or training for their service team members, to ensure the effective implementation of control measures.

（四） 审计与监督

(IV) Audit and supervision

本行应对数据安全威胁进行有效监测，实施监督检查，主动评估风险，防止数据篡改、破坏、泄露、非法利用等安全事件发生。本行每年开展 1 次涵盖个人信息保护的消费者权益保护内部专项审计，每年至少开展 1 次信息科技风险相关内部专项审计，涵盖数据安全管理、信息科技风险管理、业务连续性、系统开发及上线管理、系统运维管理等内容。

The Bank shall effectively monitor data security threats,

conduct inspection and supervision, and proactively assess risks, to prevent security incidents such as data tampering, damage, leakage, or illegal use. The Bank shall conduct annual internal specialized audit on consumer rights protection covering personal information protection, and perform special internal audits on IT related risks at least once per year, which cover data security management, IT risk management, business continuity, system development and go-live management, and system operation and maintenance management.

九、 第三方数据及隐私安全管理

IX. Third Party Data and Privacy Security Management

本行与第三方合作应严格遵守《南京银行客户个人金融信息保护工作管理办法》和《南京银行数据对外提供安全管理办法》，并制定《关于加强第三方合作机构管理中消费者权益保护工作的通知》《南京银行外包风险管理办法》等三方合作机构管理专项制度，明确将数据及隐私安全工作要求纳入合作机构管理。

The Bank shall, in cooperation with third-party institutions, strictly comply with the *Administrative Measures for the Protection of Customers' Personal Financial Information of Bank of Nanjing* and the *Safety Management Measures for External Provision of Data of Bank of Nanjing,* and establish special management policies for third party cooperations such as

the *Notice on Strengthening Consumer Rights Protection in the Management of Third-Party Cooperation Institutions* and the *Outsourcing Risk Management Measures of Bank of Nanjing*. These measures clearly incorporate data and privacy security requirements into the management of cooperation institutions.

（一） 第三方机构评估

(I) Assessment of third-party institutions

1. 通过第三方合作开展业务的，全面考察评估第三方合作机构的资质和信誉等，并将其保护个人金融信息的能力作为重要评估指标，审慎选择第三方合作机构。

1. When conducting business through third-party cooperation, the Bank shall comprehensively evaluate the qualifications, credibility, and other relevant aspects of the third-party cooperation institutions, with particular emphasis on their capability to protect personal financial information as a key assessment indicator, and exercise caution in selecting such institutions.

2. 向第三方合作机构提供本行客户个人金融信息的，事先对向第三方合作机构提供个人金融信息的必要性、安全性和合法性、对客户造成的风险以及第三方合作机构保护个人金融信息安全的能力等事项开展全面评估。未经评估或者经评估存在明显风险隐患的，不得向其提供个人金融信息。

2. Prior to providing the Bank’s customer personal financial

information to a third-party cooperation institution, the Bank shall conduct a comprehensive assessment on the necessity, security, legality, potential risks to customers, and the institution's capability to safeguard personal financial information. The Bank shall not provide personal financial information to such institutions if no assessment has been conducted or if significant risks are identified during the assessment.

（二） 客户告知与同意

(II) Customer notification and consent

除非获得本行客户的事前同意，本行不会向任何外部机构和个人提供客户的个人信息，但法律法规另有规定的除外。

The Bank shall not provide any customer personal information to external institutions or individuals without prior consent from the customer, unless otherwise required by law and regulations.

本行向第三方合作机构提供本行客户个人金融信息前，将告知客户本行提供信息的目的，第三方合作机构名称和类型，第三方合作机构收集、加工、使用个人金融信息的特定用途、范围和可能产生的后果等，并事先征得客户的明示同意。

Before providing customer personal financial information to a third-party cooperation institution, the Bank shall inform the customer of the purpose of information provided, the name and type of the third-party cooperation institution, the specific

purposes, scope, and potential consequences of the third-party's collection, processing, and use of personal financial information, and obtain the customer's explicit prior consent.

在获得客户同意后，本行仅会出于合法、正当、必要、明确的目的提供客户的个人信息，并且只会提供服务所必要的个人信息，但法律法规另有规定的除外。本行将要求信息接收方严格遵守相关法律法规及本政策要点处理客户的个人信息。

The Bank shall, upon obtaining the customer's consent, only provide personal information for lawful, legitimate, necessary, and clearly defined purposes, and only disclose the minimum amount of information necessary for the service, unless otherwise required by law and regulations. The Bank shall require the recipient to strictly comply with relevant laws, regulations, and the key points of the Bank's data security and customer information protection management policy in handling the customer's personal information.

（三） 委托处理数据管理

(III) Management of data entrusted to third parties

1. 本行涉及向第三方委托处理数据时，应当以合同协议方式约定委托处理的目的、期限、处理方式、数据范围、保护措施、双方的数据安全责任和义务。

1. When entrusting data processing to a third party, the Bank shall establish the entrusted processing purpose, duration,

processing method, data scope, protection measures, and data security responsibilities and obligations of both parties through a written contract or agreement.

2. 本行不得跨主体流动核心数据，因国家机关依法履职需要的除外。

2. The Bank shall not allow core data to flow across entities, unless otherwise required by national authorities for lawful duties.

3. 对于委托处理情形，本行应通过合同协议方式与受托方约定：

3. In case of entrusted processing, the Bank shall agree with the entrusted party through contract or agreement on the following:

（1）数据提供的目的、方式、数据范围、规模、允许存储时间；

(1) Purpose, method of provision, scope, volume, and permitted storage duration of data provided;

（2）本行和受托方的数据安全保护责任；

(2) Data security protection responsibilities of both the Bank and the entrusted party;

（3）本行和受托方的数据安全保护义务，包括但不限于：受托方应及时告知可能发生的数据泄露等重要事项，受托方应接受并配合本行对其委托处理活动进行监督，受托方在未取得本行同意时不得转委托其他主体处理数据，受托方不得对外共享数据，受托方不得加工、训练、挪用数据或采取其

他形式处理数据以谋取合同或协议约定以外的利益，受托方应在合作关系中止时及时删除数据；

(3) Data security protection obligations of both parties, include but are not limited to the following: the entrusted party shall promptly inform the Bank of any potential data breaches or other critical incidents; the entrusted party shall accept and cooperate with the Bank's supervision of the entrusted processing activities; the entrusted party shall not subcontract data processing to any other entity without the Bank's prior consent; the entrusted party shall not share data externally; the entrusted party shall not process, train, misuse, or otherwise handle data in any way to obtain benefits beyond those agreed in the contract or agreement; the entrusted party shall delete data promptly upon termination of the cooperation relationship;

（4）应当采取的安全保护措施；

(4) Appropriate security protection measures to be implemented;

（5）及时返还和删除数据的实施方式。

(5) Methods and procedures for timely return and deletion of data.

4. 本行在与第三方数据合作时应实现自身与外部的安全风险隔离，与外部机构的数据交互应当通过集中管理的外联平台或应用程序接口实施，依据“业务必需、最小权限”

原则，采取有效措施对接口设计、开发、服务、运行等进行集中安全保护管理。

4. When cooperating with third parties on data sharing, the Bank shall ensure a clear security isolation between internal and external environments. Data interaction with external institutions shall be conducted through a centrally managed external connectivity platform or application programming interfaces (APIs), following the principles of "business necessity and minimum privilege", and implementing effective and centralized security management over API design, development, service delivery, and operation.

（四） 第三方机构监督与检查

(IV) Supervision and inspection by third-party institutions

1. 对于委托处理情形，本行应有效监督受托方的履约情况，每年评估确认：受托方是否具备足够的数据安全保护能力；受托方的数据处理活动是否符合事前约定；受托方是否已采取承诺的全部安全保护措施等内容。

1. For entrusted processing scenarios, the Bank shall effectively monitor the performance of the trustee and conduct annual assessments to confirm: whether the trustee possesses adequate data security protection capabilities; whether the trustee’s data processing activities comply with prior agreements;

and whether the trustee has implemented all committed security protection measures.

2. 本行应每年对数据提供单位的数据对外提供行为进行检查，检查内容包括但不限于评估流程的落实情况、数据安全保护措施的落实情况、评估记录的保存情况等。

2. The Bank shall conduct annual inspections of data provision activities by data-providing entities. The inspection scope shall include, but is not limited to, the implementation of assessment procedures, the implementation of data security measures, and the retention of assessment records.

十、 客户对其个人信息控制的权利

X. Customer's Right to Control its Personal Information

个人客户中心系统是本行统一管理和存储个人客户基础信息的核心系统，并向本行各系统提供个人客户基础信息的各类服务：具体包括查询使用、存储、修改、删除、备份等。

The personal customer information management system is the core system of the Bank for centralized management and storage of basic personal customer information, which provides various services for the Bank's systems on basic personal customer information, including query and usage, storage, modification, deletion and backup.

（一）查阅权

(I) Right to access

个人客户有权向本行查阅、复制其个人信息，本行各级机构应当及时提供，但法律、行政法规规定应当保密或者不需要告知的情形除外。个人客户死亡的，其近亲属为了自身的合法、正当利益，可以对死者的相关个人信息行使查阅、复制、更正、删除等权利，死者生前另有安排的除外。

Personal customers have the right to access and copy their personal information from the Bank, and entities at all levels of the Bank shall provide such information in a timely manner, except for circumstances where laws and administrative regulations require confidentiality or do not require disclosure. In the event of the death of a personal customer, their close relatives may, for their own legitimate and proper interests, exercise the rights of viewing, copying, correcting, and deleting the relevant personal information of the deceased, unless the deceased had made other arrangements before their death.

（二）更正权

(II) Right to correct

个人客户发现其个人信息不准确或者不完整的，有权请求本行更正、补充。本行各级机构应当对其个人信息予以核实，并及时更正、补充。客户可通过手机银行等渠道自行修改、更新个人信息，还可以通过本行网点等渠道提出修改申

请。

Where a personal customer notes that their personal information is inaccurate or incomplete, they have the right to request the Bank to correct or supplement it. The Bank's entities at all levels shall verify their personal information obtained, correct and supplement it in a timely manner. Customers can modify and update their personal information through channels such as mobile banking, or submit modification requests through the Bank's business outlets.

（三）删除权

(III) Right to delete

客户可在具备信息删除权限的系统或渠道要求删除其部分个人客户信息要素，相关系统或渠道主管部门需在明确告知信息删除的影响后予以响应。如所需删除信息为反洗钱等法律、行政法规要求金融机构必须留存或办理已有业务所必须，暂时无法删除的，需向客户明确告知。

When a customer requests to delete certain personal customer information elements in a system or channel with information deletion authority, the relevant system or channel's responsible department shall respond after clearly informing the customer of the impact of the deletion. If the information to be deleted is required by laws and administrative regulations such as

anti-money laundering to be retained by financial institutions or is necessary for ongoing business transactions, and cannot be deleted for the time being, this shall be clearly communicated to the customer.

十一、 检视与更新

XI. Review and Update

本行将根据国家政策、监管要求、行业发展和内部管理需要，适时对本制度进行检视和更新。

Bank of Nanjing will periodically review and update the policy in accordance with national policies, regulatory requirements, industry development and internal operational needs.