隐私和数据安全

Privacy and Data Security

本行严格落实《中华人民共和国网络安全法》、《中华人民共和国个人信息保护法》、《中华人民共和国数据安全法》、《党委（党组）网络安全工作责任制实施办法》要求，明确党委、董事会对本行网络安全与数据安全工作负主体责任，董事会战略规划与可持续发展委员会承担审议重大数据治理事项，并向董事会提出建议的职责。董事长为本行网络安全与数据安全第一责任人，各级机构分管网络安全与数据安全的行长为直接责任人，每年向高管层报告网络安全与数据安全管理工作和责任落实情况。

The Bank strictly implements the requirements of the *Cybersecurity Law of the People's Republic of China*, the *Personal Information Protection Law of the People's Republic of China*, the *Data Security Law of the People's Republic of China* and the *Measures for the Implementation of the Responsibility System for Cybersecurity Work of the Party Committee (Party Group)*, and specifies that the Party Committee and the Board of Directors are responsible for cybersecurity and data security of the Bank, and the Board's Strategic Planning and Sustainable Development Committee is responsible for reviewing major data governance matters, and presenting recommendations to the Board. The Chairman of the Board is the first responsible person for cybersecurity and data security of the Bank, and the presidents of the institutions at all levels in charge of cybersecurity and data security are the direct responsible persons, and report the cybersecurity and data security management work and responsibility implementation to the senior management every year.

管理架构

Management Structure

纵向实行层级负责制。明确党委、董事会对本行网络安全与数据安全工作负主体责任，本行主要负责人为数据安全第一责任人，分管数据安全的高级管理人员为直接责任人。每年向本行党委、董事会、高管层报告网络安全与数据安全管理工作和责任落实情况。

A vertical hierarchical responsibility mechanism is implemented. The Party Committee and the Board of Directors bear the primary responsibility for cybersecurity and data security of the Bank. The Bank's principal responsible person is the first accountable person for data security, and the senior management member in charge of data security is the direct responsible person. An annual report on cybersecurity and data security management work and the implementation of responsibilities is submitted to the bank’s Party Committee, Board of Directors, and senior management.

横向实行条线管理制。按照“谁管业务、谁管业务数据、谁管数据安全”，以及“系统谁主管、保护谁牵头”，“数据谁使用、责任谁承担”的原则，各部门负责本条线数据安全管理工作，主要负责人是本部门数据安全管理的第一责任人，分管数据安全的领导负直接管理责任。

A horizontal line management mechanism is implemented. Each department is responsible for data security management within its respective business line in accordance with the principles that “the person who manages business is responsible for the business data and data security”, “the person in charge of the system is also in charge of system protection” and "the person who uses data

shall also bear the corresponding responsibility". The main responsible person is also the first responsible person for data security of the department, and the leader in charge of data security assumes direct management responsibility.

管理制度体系

Management System

本行持续建立健全数据安全管理制度体系，构建覆盖数据全生命周期和应用场景的安全保护机制，保障各项数据开发利用活动安全稳健开展。报告期内，本行紧跟国家法律法规、监管规定，修订《数据安全管理办法》，并以《数据安全管理办法》为基础制度，配套制定《数据分类分级工作指引》、《数据安全通用保护规范》、《数据出行安全管理工作指引》、《数据安全事件应急预案》、《关于加强数据安全评估工作的指导意见》、《办公终端数据安全管理工作指引》等细分领域规范标，确保各项新要求有效内化。

The Bank continued to improve the data security management system, built a security protection mechanism that covers the entire life cycle of data and key application scenarios to ensure safe and sound implementation of various data development and application activities. During the reporting period, in strict compliance with national laws and regulations, and supervisory provisions, we revised the *Data Security Management Measures*, and formulated supporting regulations in specific areas, such as the *Guidelines for Data Classification and Grading*, the *General Data Security Protection Standard*, the *Guidelines for Data Export Security Management*, the *Data Security Incident Emergency Response Plan*, the *Guiding Opinions on Strengthening Data Security Assessment*, and the *Guidelines for Data Security Management of Office Terminals* on the basis of

the *Data Security Management Measures* to ensure that new requirements are effectively implemented.

持续强化数据安全集团一体化管理，在各境外机构和各子公司建立数据安全管理机制，设立专门机构或专人负责数据安全工作。本行数据安全政策范围覆盖境内各级机构全部业务条线及境外分行，境外分行同时遵守驻在地法律、法规和监管要求，按照孰严原则执行。报告期内，召开年度全集团数据安全工作会议部署工作任务，按机构类型开展差异化解读，推动各境外机构及子公司建立健全数据安全治理架构，制定数据安全管理制度，明确岗位职责与工作机制，提升集团一体化数据安全管理水平。

The integrated management of data security across the Group was continuously strengthened. All overseas institutions and subsidiaries established their data security management mechanisms, designated specialized organizations or individuals responsible for data security. The Bank's data security policies apply to all business lines of domestic institutions at all levels, and overseas branches. Overseas branches shall also comply with laws, regulations and supervisory requirements of the countries where they operate, and implement the stricter requirements where differences exist. During the reporting period, we held annual group-wide data security work conference to assign tasks, tailored the implementation of the tasks based on types of institutions, and motivated overseas institutions and subsidiaries to establish and improve data security governance structures, formulate data security management system, and define job responsibilities and work mechanisms, thus improving integrated data security management across the Group.

本行公开披露《数据安全与客户信息保护管理政策要点》[1]，系统展示本行客户信息保护相关政策的制度框架，重点涵盖原则、组织架构、个人客户信息的收集和使用的管理措施等。

We publicly disclosed the *Key Points of Data Security and Customer Information Protection Management Policy of Agricultural Bank of China*, which systematically outlines the framework of the Bank's policies on customer information protection, focusing on key areas such as guiding principles, organizational structure, and management measures for the collection and use of personal customer information.

个人信息的收集和使用目的包括：提供并改进金融产品或服务，识别和验证客户身份，审批、管理、执行客户授权的交易；履行合规义务，包括监管、税务及其他法律要求，并根据境内外法规向有关部门报告（如反洗钱、反恐融资、反腐败、逃税、欺诈等）；在提供金融服务期间，客户同意本行依法及依约定持续处理其个人信息；客户注销服务后，本行将停止收集信息，但根据法律法规，可在资料归档、审计、监管协查及履行反洗钱和制裁义务等情形下继续使用已收集的信息；为优化服务体验或防控风险，本行可能对服务使用情况进行汇总、统计和分析，但不包含个人身份识别信息；为使客户了解其服务使用情况或介绍本行相关服务，可能发送服务通知及商业信息；其他经客户授权或法律允许的用途。

Purposes of collecting and using personal information: Providing and improving financial products and services, identifying and verifying customer identities, and reviewing, managing, and executing transactions authorized by customers; fulfilling compliance obligations, including

[1] 敬请参阅本公司官方网站“农行 ESG-政策要点”栏目发布的《中国农业银行数据安全与客户信息保护管理政策要点》：P020250626658744793012.pdf

regulatory, tax, and other legal requirements, and reporting matters related to anti-money laundering, counter-terrorism financing, anti-corruption, tax evasion, and fraud to relevant authorities in accordance with domestic and foreign laws and regulations. During the provision of financial services, the customer gives consent to the Bank's ongoing processing of their personal information in accordance with applicable laws and agreed terms. After the customer cancels the service, the Bank will cease collecting personal information, but may continue to use previously collected information in accordance with applicable laws and regulations for purposes such as record archiving, auditing, regulatory investigations, and fulfilling anti-money laundering and sanctions obligations. To enhance service experience or manage risks, the Bank may aggregate, compile statistics, and conduct analysis on the use of services, but such processing will not include personally identifiable information. To help customers understand their use of services or to introduce relevant services offered by the Bank, we may send service notifications and commercial information. Personal information is also collected and used for other purposes permitted by law or authorized by the customer.

第三方可访问数据及其使用目的：本行与第三方各自独立决定个人信息的处理目的和方式。当本行向第三方提供个人客户信息时，将告知客户接收方的身份、联系方式、处理目的和方式、信息种类，并取得客户单独同意；同时与第三方约定处理范围并监督其合规操作，如第三方变更处理方式，须重新取得客户同意。对于外包、合作或中介服务中涉及个人信息处理的，本行将评估第三方的数据保护能力，并在协议中明确双方责任，监督其履行义务。向第三方提供敏感数据前，本行将取得客户同意，并通过合同明确处理目的、范围、留存期限及安全责任。委托第三方处理敏感数据的，须通过协议明确处理方式、数据范围、保护措施、安全责任及数据返还或删除方式，严禁第三方擅自转委托或用于其他用途。本行持续监督第三方的数据处理行

为，严格控制数据对外提供，实行清单制管理，并依据《数据出行安全管理工作指引》落实数据安全评估、审批流程及应急处置机制。

Data access by third parties and the purpose: The Bank and third parties independently determine the purposes and methods of processing personal information. When we provide personal customer information to third parties, we inform the customer of the recipient's identity, contact details, purpose and method of processing, as well as the categories of information involved, and obtain the customer's separate consent. We also define the scope of processing with third parties through agreements and supervise relevant compliance procedures. If third parties change the processing method, we obtain the customer's consent again. Where personal information processing is involved in outsourcing, cooperation or intermediary services, we assess the data protection capabilities of the third parties, clearly define respective responsibilities in the agreement, and supervise their fulfillment of obligations. Prior to disclosing sensitive data to third parties, we obtain the customer's consent and specify the purpose, scope, retention period, and security responsibilities through contracts. When entrusting third parties to process sensitive data, we clearly define the processing methods, data scope, protective measures, security responsibilities, and data return or deletion methods through written agreements. Third parties are strictly prohibited from delegating data processing or using the data for unauthorized purposes. We continue to monitor data processing activities by third-parties, strictly control the disclosure of data to external parties, adopt a list-based management approach, and follow the *Guidelines for Data Export Security Management* to enforce data security assessments, approval procedures, and emergency response mechanisms.

数据分类分级管理

Data Classification and Grading Management

本行制定数据分类分级相关制度，明确数据分类分级原则性要求、动态调整审批机制和实施操作流程，针对不同安全级别的数据，结合数据安全通用保护要求，明确数据全生命周期差异化安全保护措施，统筹兼顾数据安全保护和数据合理使用。自主研发数据分类分级工具，借助专家模型等方式支撑数据自动化标识。

The Bank formulated policies for data classification and grading, to clarify the principle-based requirements, dynamic adjustment and approval mechanisms, and implementation procedures for classification and grading. We specified the differentiated protection measures for the entire life cycle of data, following the general protection requirements for data security, and made overall plans for data security protection and rational use of data. We developed in-house data classification and grading tools to enable automated data labeling via expert models and other methods.

数据最小化收集和留存

Minimal Data Collection and Retention

- 客户信息收集
- **Collection of Customer Information**

全面贯彻国家金融监督管理总局《商业银行代理销售业务管理办法》、《金融机构产品适当性管理办法》及《关于进一步加强金融机构营销行为管理的通知》等最新监管要求，报告期

内，本行修订《中国农业银行零售营销宣传行为管理办法》，单列“信息保护”条款，明确“最小必要”原则、同意撤回机制、查询权限清单及泄露事件报告路径，全面提升客户信息合规水平。本行收集客户信息遵循合法、正当、必要、诚信原则，在限于实现处理目的的最小范围内，按照法律、行政法规要求和业务需要收集客户信息，不收集与业务或所提供服务不直接相关的信息，不采取不正当方式收集客户信息。

The Bank fully implements the latest regulatory requirements of the by National Financial Regulatory Administration, such as the *Administrative Measures for Agency Sales Business of Commercial Banks*, the Administrative Measures for Product Suitability of Financial Institutions and the *Notice on Further Strengthening the Management of Marketing Activities of Financial Institutions*. During the reporting period, we revised the *Administrative Measures for Retail Marketing and Promotion Activities of Agricultural Bank of China*, with a separate provision on “Information Protection”. The revision clarifies the principle of “minimum necessity”, the mechanism for withdrawal of consent, list of access rights, and reporting pathways for data breach incidents, thereby comprehensively enhancing the compliance of customer information management. We collect customer information in accordance with the principles of legality, legitimacy, necessity, and integrity. Within the minimum scope necessary to achieve the processing purposes, customer information is collected in compliance with laws, administrative regulations, and business needs. Information not directly related to the business or services provided is not collected, and improper means is not used to obtain customer information.

本行公开收集规则，明示收集信息的目的、方式、范围、保存期限以及同意收集信息的可能后果，并经被收集者同意。个人信息的处理目的、处理方式和处理的个人信息种类发生变更的，将重新取得个人同意。

The Bank publicly discloses its collection rules, specifying the purpose, method, scope, retention period of the information collected, and the possible consequences of consenting to the collection, and obtains the consent of the individuals concerned. In case of changes to the purpose, method, or type of personal information processed, new consent from the individuals is obtained.

收集客户信息前，主动履行“告知-同意”义务。通过隐私政策、产品（服务）协议、授权书等渠道，以显著标识和通俗语言明确告知客户个人信息的收集目的、使用方式、范围及保存期限，依法取得客户授权或单独同意。

Before collecting customer information, we fulfill the "notice and consent" requirement in a proactive manner. We use prominent markings and plain language in privacy policies, product or service agreements, and authorization letters, etc. to clearly inform customers of the purpose, use, scope and retention period of the personal information that we will obtain, and ensure that customer authorization or separate consent is obtained in accordance with the law.

收集客户信息时，要求第三方说明客户信息来源，对其客户信息来源的合法性进行确认；了解第三方已获得的客户信息处理的授权同意范围，包括使用目的，信息主体是否授权同意共享、转让、公开披露、跨境流动等；如开展业务需进行的客户信息处理活动超出第三方获得的同意范围，需要在获取客户信息后的合理期限内或处理客户信息前，征得信息主体的明示同意。

When collecting customer information from any third party, we require the third party to disclose the source of the information and confirm its legality. We also verify the scope of authorization and consent obtained by the third party for processing the customer information, including the purpose of usage, and whether the information subject authorized the sharing, transfer, public disclosure, and cross-border transfer of such information. If the customer information processing activities required for business operations exceed the scope of consent obtained by the third party, explicit consent from the information subject must be obtained within a reasonable period after obtaining the customer information or before processing it.

- 客户信息使用
- **Usage of Customer Information**

本行使用客户信息时，严格按照收集该信息的目的，且不超过客户授权的使用范围；通过接入征信系统、支付系统及其他系统获取的客户信息，严格按照有关规定或约定的用途使用。

When using customer information, the Bank strictly adheres to the purposes for which the information is collected and does not exceed the scope authorized by the customers. Customer information obtained through access to credit reporting systems, payment systems, and other systems is used strictly in accordance with relevant regulations or agreed-upon purposes.

- 客户信息留存
- **Retention of Customer Information**

本行在符合法律法规和监管规定的情况下，对客户个人信息进行删除或作匿名化处理，尤其是个人客户信息的存储期限维持在最小必要限度内。

In compliance with laws, regulations, and regulatory requirements, the Bank deletes or anonymizes customer personal information. In particular, the storage period for personal customer information is kept to the minimum necessary limit.

留存规定 **Retention requirements**	留存时限 **Retention periods**
反洗钱工作相关信息的保存 **Retention of information related to anti-money laundering activities**	本行执行《中国农业银行反洗钱工作基本规范》，反洗钱相关客户身份资料在业务关系结束后、客户交易信息在交易结束后，至少保存 10 年，监管另有更严规定的，从其规定。 The Bank implements the *Basic Norms for Anti-Money Laundering Work of Agricultural Bank of China*. Customer identification records are retained for at least 10 years after the termination of the business relationship, and transaction records are retained for at least 10 years after the transaction date. Where regulatory requirements prescribe a longer retention period, the Bank follows the stricter provisions.

基金代销规定 **Requirements on distribution of funds**	本行各级机构根据《中国农业银行公募证券投资基金代理销售业务管理办法》的规定，妥善保管基金份额持有人的开户资料和销售业务有关资料。投资人身份资料自业务关系结束当年计起至少保存 20 年，与基金销售业务有关的其他资料自业务发生当年计起至少保存 20 年。 In accordance with the *Management Measures for Agency Sales of Publicly Offered Securities Investment Funds of Agricultural Bank of China*, all levels of the Bank properly retain records related to fund account opening and sales activities. Investor identification documents are retained for at least 20 years from the year the business relationship ends, and other records related to fund sales are retained for at least 20 years from the year the relevant business activity occurs.
理财产品代销规定 **Requirements on distribution of wealth management products**	本行制定《中国农业银行理财产品代理销售业务管理办法》，规定理财产品销售相关资料，保管年限不低于 20 年。 The Bank has established the *Management Measures for Agency Sales of Wealth Management Products of Agricultural Bank of China*, which stipulate that related sales records must be retained for no less than 20 years.

银行卡收单规定 **Requirements on bank card acquiring services**	根据《中国农业银行收单业务管理办法》，本行开办收单业务的各级机构做好特约商户档案资料管理，档案资料包括特约商户申请材料、资质审核材料、受理协议、培训和检查记录、信息变更、终止服务等档案资料。本行以必要措施保存特约商户档案资料和交易记录，至少保存至收单服务终止后 5 年，其中特约商户身份资料和交易记录至少保存 10 年。 Pursuant to the *Administrative Measures for Acquiring Business of Agricultural Bank of China*, all levels of the Bank that conduct acquiring business are responsible for managing the records of contracted merchants. These records include application documents, qualification review materials, acceptance agreements, training and inspection records, information changes, and service termination records. The Bank takes necessary measures to retain contracted merchant records and transaction data for at least five years after the termination of the acquiring service. Contracted merchant identification documents and transaction records are retained for at least 10 years.

网络安全

Cybersecurity

本行数据中心引入 ISO27001 国际标准并通过认证，建立覆盖全面的标准化信息安全管理体系，连续多年顺利通过中国网络安全审查认证和市场监管大数据中心（CCRC）认证审核。建立 7×24 小时监控值班机制，实施网络安全事件分类分级管理，建立常态化安全应急机制，形成漏洞治理闭环管理流程。实现项目研发全生命周期安全管控，推动 SDL 标准与研发过程相融合。

The Bank's data center adopted widely accepted standards such as the ISO27001 with related certification, and established a comprehensive and standardized information security management system. For several consecutive years, we successfully passed the certification audits of the China Cybersecurity Review and Market Regulation Big Data Center (CCRC). We established a 24/7 monitoring and on-duty mechanism, implemented classified and graded management for cybersecurity incidents, and developed a normalized security emergency response mechanism, forming a closed-loop vulnerability management process. We achieved full-lifecycle security control in project research and development, promoting the integration of SDL standards with R&D.

客户隐私保护

Customer Privacy Protection

- 制度建设
- **Policy Development**

本行制定《客户信息保护管理办法》《对公客户信息保护实施细则》、《个人客户信息保护实施细则》等专项个人信息保护制度，保护客户信息安全。制定《个人信息保护审查指引》《个人信息保护工作指引》、《个人信息保护事前影响评估工作指引》，细化个人信息保护操作性规范。同时，将个人信息保护的具体要求纳入各项业务制度，推动合同变更、制度修订、数据管控、系统改造同步治理，将个人信息保护要求贯穿到业务经营和客户服务的全流程、各环节。

We formulated special personal information protection policies, including the *Management Measures for Customer Information Protection*, the *Implementing Rules for the Protection of Corporate Customer Information* and the *Implementation Rules for the Protection of Personal Customer Information* applicable to corporate business to safeguard the information security of customers. We also formulated the *Personal Information Protection Review Guidelines*, the *Personal Information Protection Guidelines* and the *Guidelines for Prior Assessment of Personal Information Protection Impact*, to specify the operational standards for personal information protection. Meanwhile, we integrated specific requirements for personal information protection into all relevant business policies. In doing so, we intend to promote synchronous governance in contract modifications, regulation revisions, data control, and system upgrades, integrating personal information protection requirements into all the processes and links of business operations and customer service.

本行高度重视并切实保障个人信息主体权利,严格落实《中华人民共和国个人信息保护法》、《中华人民共和国消费者权益保护法》、《中华人民共和国网络安全法》、《中华人民共和国数据安全法》等法律法规和监管要求，持续加强客户个人隐私保护工作，制定《隐私政策（对

公版）》、《隐私政策（个人版）》等个人信息处理规则，并通过官网、掌上银行、柜面、超级柜台等线上线下渠道同步发布，依法公开客户个人信息处理规则。建立动态监测机制，持续跟踪最新的法律法规及监管要求，及时完成制度修订与版本迭代。We attach great importance to the protection of data subject rights and strictly comply with relevant laws and regulations, including the *Personal Information Protection 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 *Cybersecurity Law of the People's Republic of China*, and the *Data Security Law of the People's Republic of China*, as well as other regulatory requirements. We continued to strengthen the protection of customer privacy, and formulated personal information processing rules such as *Privacy Policy (Corporate Version)* and *Privacy Policy (Individual Version)*, and published them simultaneously on online and offline channels such as official websites, mobile banks, counters, and super counters to disclose personal information processing rules in accordance with the law. We established a dynamic monitoring mechanism to continuously track the latest laws, regulations, and regulatory requirements, and promptly complete policy updates and version iterations.

- **具体措施**
- **Specific Measures**

严格执行分级授权机制。根据客户信息的重要性、敏感度及业务开展需要，合理确定工作人员、主管系统使用信息的范围、权限及程序。

Strictly implementing a hierarchical authorization mechanism. We properly determined the scope, authority, and procedures for staff and supervisors to use information based on the importance and sensitivity of customer information, as well as business needs.

建立客户个人信息保护全流程管理体系。实施事前影响评估机制，完善系统与制度建设，将个人信息保护纳入监督检查重点，强化风险防控，切实保障客户信息安全。组织开展年度个人信息保护风险专项排查，涵盖违规收集、查询、存储、使用、传输个人信息等 8 类重点风险场景。

Establishing an end-to-end management system for customer personal information protection. We implemented a pre-implementation impact assessment mechanism to improve systems and policy frameworks, incorporated personal information protection into the key areas of supervision and inspections to strengthen risk prevention and control, and to ensure the security of customer information. We organized special initiative to identify personal information protection risks on an annual basis, covering eight key risk scenarios including unauthorized collection, access, storage, use, and transmission of personal information.

主动履行“告知-同意”义务依规处理个人信息。通过隐私政策、产品（服务）协议、授权书等渠道，以显著标识和通俗语言明确告知客户个人信息的收集目的、使用方式、范围及保存期限，依法取得客户授权或单独同意。严格依规处理个人信息，杜绝篡改或违法使用行为，采取有效措施防止个人信息被滥用、非法使用、泄露或出售，切实保障信息安全。

Proactively fulfilling the "notice and consent" requirement in processing personal information according to regulations. We use prominent markings and plain language in privacy policies, product or service agreements, and authorization letters, etc. to clearly inform customers of the purpose, use, scope and retention period of the personal information that we will obtain, and ensure that customer authorization or separate consent is obtained in accordance with the law. We strictly process personal information in accordance with regulations, and prohibit any unauthorized

modification or illegal use. We also take effective measures to prevent the misuse, illegal use, disclosure, or sale of personal information, thereby ensuring information security.

深度融合个人信息保护要求与数据安全评估。针对处理敏感个人信息、对外提供个人信息、自动化决策等情形，积极开展个人信息保护事前影响评估。根据数据处理目的、性质及范围，结合法律法规与伦理规范，系统分析数据安全风险及其对数据主体权益的影响，重点评估数据处理的必要性、合规性，以及风险防控措施的有效性。针对识别出的风险，通过管理措施（如访问控制、身份管理）与技术手段（如数据加密、脱敏及风险监测审计），验证保护措施的有效性。

Deeply integrating personal information protection requirements into data security assessment. For scenarios involving the processing of sensitive personal information, providing personal information to external parties, and the use of automated decision-making, we actively implement pre-implementation impact assessment on personal information protection. Based on the purpose, nature, and scope of data processing, we systematically analyze data security risks and their impact on data subject rights in accordance with applicable laws, regulations, and ethical standards. The assessment focuses on the necessity and compliance of data processing, as well as the effectiveness of risk mitigation measures. For identified risks, we verify the effectiveness of protection measures through management measures, such as access control and identity management, and technical means, such as data encryption, desensitization and risk monitoring audit.

尊重和保障客户在个人信息处理活动中权利。

Respecting and protecting customers' rights in personal information processing activities.

查阅权：客户可通过本行网点、网银、掌上银行等渠道查询、访问客户个人信息。

Right to access: Customers can inquire and access their personal information through the Bank's business outlets, online banking, mobile banking app and other channels.

更正权：客户可通过网银、掌上银行等渠道自行修改、更新个人信息，还可以通过本行网点、客服热线（95599）等渠道提出修改申请。

Right to rectify: Customers can modify and update their personal information through online banking, mobile banking app and other channels, or submit modification requests through the Bank's business outlets and the customer service hotline (95599).

删除权：客户对其个人信息享有删除权，客户通过网点、客服热线（95599）等渠道依法申请在日常业务功能所涉及的系统中删除本人个人信息。

Right to delete: Customers have the right to delete their personal information. They can apply through business outlets and the customer service hotline (95599) to delete their personal information from systems involved in regular business functions.

第三方数据及隐私安全管理

Third-Party Data and Privacy Security Management

- **采购流程中对第三方数据及隐私安全管理**
- **Third-party data and privacy security management in the procurement process**

本行在《中国农业银行集中采购平台供应商注册协议》、《中国农业银行农银 e 采平台操作规程》等协议、制度、招标文件及采购流程的多个环节，明确供应商在数据安全方面的责任与义务，确保数据处理过程的合规与安全，切实保障本行及本行客户的合法权益。

We clearly outline suppliers' responsibilities and obligations regarding data security, ensuring compliance and security in data processing and effectively safeguarding the legitimate rights and interests of the Bank and its clients through agreements such as the *Supplier Registration Agreement for the Centralized Purchasing Platform of Agricultural Bank of China* and the *E-procurement Platform Operation Procedures of Agricultural Bank of China*, as well as related policies, tender documents, and procurement workflows.

引入供应商前

Prior to selecting suppliers

在招标文件中明确要求投标人须承担的保密义务，不得将招标获得的信息向第三方外传。在注册采购平台时，供应商须接受注册协议中的保密条款，对本行相关数据或信息承担保密义务。在平台操作规程中明确提出任何单位和个人不得伪造、篡改或者损毁电子招采活动信息，其他系统在采集、汇总、传输、存储、公开、使用采购平台数据过程中加强数据安全管理。在电子招投标平台中引入第三方数字身份认证证书加密机制，确保电子招投标过程真实有效、抗抵赖、可追溯。

Bidding documents explicitly stipulate the confidentiality obligations for bidders, prohibiting the disclosure of information obtained through bidding to any third party. When registering on the procurement platform, suppliers must accept the confidentiality clauses in the registration agreement

and undertake confidentiality obligations for the Bank's related data or information. In the platform operating procedures, it is explicitly stated that no entity or individual is allowed to forge, alter, or destroy information related to electronic procurement activities. In addition, other systems involved in the collection, aggregation, transmission, storage, disclosure, or use of data from the procurement platform shall strengthen data security management throughout the process. A third-party digital identity authentication certificate encryption mechanism is introduced into the electronic bidding platform to ensure authenticity, non-repudiation, and traceability of the electronic bidding process.

确定中选供应商后

After suppliers are selected

制定规范合同条款，明确界定供采双方在本行及本行客户信息保护方面的责任和义务。实施严格的安全管控措施，要求供应商妥善保管记载客户信息的载体，对涉及本行客户或经营信息的系统，严格按照有关要求执行查询、审批流程，规范密码使用，做到操作合规和信息保密。

Standardized contract terms are formulated to clearly define the responsibilities and obligations of both parties in terms of customer information protection for the Bank and its customers. Stringent security control measures are implemented, requiring suppliers to properly store carriers containing customer information and strictly comply with relevant requirements for inquiry and approval processes for systems involving the Bank's customers or operational information, standardizing password use to ensure operational compliance and information confidentiality.

- 加强从第三方获取客户信息的管理

- **Enhancing the management of customer information obtained from third parties**

严禁将客户个人隐私数据出租、出售或提供给第三方作为完成交易或服务以外的用途。本行严格遵守法律法规和相关管监管要求，对业务过程中知悉的客户信息予以保密，采取有效措施加强对客户信息的保护，依法使用工作中获取的客户信息，不得以任何形式：（1）出售客户信息（2）向本行以外的其他机构或个人等第三方提供客户信息，但为客户办理相关业务所必需并经客户本人书面授权或单独同意的，以及法律法规和监管部门另有规定的除外。

Strictly prohibiting the renting, selling, or providing of customer privacy data to third parties for purposes other than transactions or services. The Bank strictly complies with laws, regulations, and relevant supervisory requirements, keeps confidential customer information obtained in the course of business, takes effective measures to strengthen the protection of customer information and uses such information in accordance with the law. Under no circumstances shall customer information be: (1) sold; (2) provided to any other institution or individual other than the Bank, except where such disclosure is necessary for the purpose of processing a transaction on behalf of the customer and has been expressly authorized or separately consented to in writing by the customer, or as otherwise provided by laws, regulations, or regulatory authorities.

明确从第三方获取客户信息的要求。制定《客户信息保护管理办法》，明确从第三方获取客户信息时，要求第三方说明客户信息来源，对其客户信息来源的合法性进行确认；了解第三方已获得的客户信息处理的授权同意范围，包括使用目的，信息主体是否授权同意共享、转让、公开披露、跨境流动等；如开展业务需进行的客户信息处理活动超出第三方获得的同意范围，需要在获取客户信息后的合理期限内或处理客户信息前，征得信息主体的明示同意。

Clarifying the requirements for obtaining customer information from third parties. The Bank formulated the *Management Measures for Customer Information Protection*, making clear that when obtaining customer information from any third party, the Bank shall require the third party to disclose the source of the information and confirm its legality. The Bank shall also verify the scope of authorization and consent obtained by the third party for processing the customer information, including the purpose of usage, and whether the information subject authorized the sharing, transfer, public disclosure, and cross-border transfer of such information. If the customer information processing activities required for business operations exceed the scope of consent obtained by the third party, explicit consent from the information subject must be obtained within a reasonable period after obtaining the customer information or before processing it.

确保外部数据信息合法真实。将外部数据采购与合作引入纳入外包风险管理体系。制定《外部资讯服务管理办法》，建立覆盖需求收集、安全评估、数据接入、运维管理、登记备案及监督评价的闭环管理机制，重点核查数据来源真实性与合法性，评估数据提供方的安全保障能力及潜在风险，并通过协议明确双方数据安全责任。外部数据使用部门对其数据应用的安全管理承担主体责任，并采取恰当措施保障数据安全合规使用。

Ensuring the legality and authenticity of data from external sources. We incorporated procurement and use of external data into the outsourcing risk management framework. We formulated the *Administrative Measures for External Information Services*, established a closed-loop management mechanism that covers the entire life cycle of external data, including demand collection, security assessment, data integration, operations management, registration and filing, as well as supervision and evaluation, focusing on verifying the authenticity and legality of data sources,

assessing the data provider's capability in data security and potential risks, and defining data security responsibilities of both parties through contractual agreements. The department using external data is responsible for the relevant security management, and shall implement appropriate measures to ensure the secure and compliant use of data.

- **严格管理向第三方提供的客户信息**

- **Strict management of customer information provided to third parties**

本行严格管控向第三方提供数据，制定发布《客户信息保护管理办法》、《数据出行安全管理工作指引》，相关场景实施清单制管理，明确数据安全评估、审查审批机制流程，规范第三方机构管理、合同协议约束和事件应急处置。对于业务中需要向第三方提供敏感数据的，本行会取得客户同意，涉及个人信息的，告知客户接收方的名称、联系方式、处理目的、保存期限、处理方式和个人信息的种类，并取得个人的单独同意；采取必要的管理和技术手段，确保实施过程安全；并与第三方机构以合同协议等方式约定数据提供的目的、范围、接收方数据留存时限、明确数据责任与义务。对于委托处理第三方处理敏感数据的，会以合同协议签方式与第三方约定委托处理目的、期限、处理方式、数据范围、个人信息种类、保护措施、受托方重大事项报告、委托方和受托方的数据安全责任、义务和权利，以及受托方返还或删除数据的方式等，要求未经本行同意，第三方不得转委托其他主体处理数据,不得对外共享数据，不得加工、训练、挪用数据，或者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。在合作过程中，对第三方数据处理活动进行监督。

The Bank strictly controls the provision of data to third parties. We developed the *Management Measures for Customer Information Protection* and the *Guidelines for Data Export Security*

Management, implemented list-based management approach for certain circumstances, clarified the process of data security assessment, review and approval mechanism, and standardized the management of third-party institutions, contract constraints and emergency response to incidents. Where sensitive data needs to be provided to third parties in the course of business, we obtain customer consent. If the data involves personal information, we inform the customer of the recipient's name, contact details, purpose and duration of processing, processing methods, and categories of personal information involved, and obtain the individual's separate consent. Additionally, we take necessary management and technical measures to ensure secure processing, and clearly define the purpose, scope, data retention period of the recipient, and respective data responsibilities and obligations with the third parties through contractual agreements. When engaging third parties to process sensitive data, we enter into contractual agreements with the third party to specify the purpose, duration, processing methods, data scope, categories of personal information, protection measures, report on material matters of the engaged party, and the respective data security responsibilities, obligations, and rights of both parties, as well as the methods for data return or deletion. The third party is strictly prohibited from delegating the processing to any other party, sharing the data externally, processing, training, or misappropriating the data, or using the data in any other manner for purposes beyond those agreed upon in the contract or agreement. We supervise the data processing activities of third parties during the engagement.

- 监督第三方保护个人客户信息

- **Supervision over third parties in protecting customers' personal information**

明确第三方使用个人客户信息的要求。本行制定《个人客户信息保护实施细则》，明确开展外包活动、对外开展业务合作、聘请中介机构提供服务时，涉及与第三方合作处理个人客户信息的，应充分审查、评估第三方保护个人客户信息的能力，根据法律法规和制度规定在业务合作协议或保密协议中具体明确双方在保护个人客户信息方面的职责和义务，并采取必要措施监督第三方履行上述职责和义务，准确记录和储存与第三方合作处理个人客户信息的情况。

Clarifying the requirements for using customers' personal information by third parties. The Bank formulated the *Implementation Rules for the Protection of Personal Customer Information*, specifying that when outsourcing, conducting business cooperation, or engaging intermediaries to provide services involve processing customers' personal information with any third party, the Bank shall thoroughly review and assess the third party's ability to protect customers' personal information; specify the responsibilities and obligations of both parties in protecting customers' personal information in business cooperation agreements or confidentiality agreements in accordance with laws, regulations, policies and rules, take necessary measures to supervise the third party's fulfillment of these responsibilities and obligations, and accurately record and store information related to processing customers' personal information in cooperation with the third party.

与第三方机构开展数据合作时。本行制定《数据安全管理办法》，在与第三方机构开展数据合作时，严格实现内外部风险隔离，通过集中管理的外联平台或应用程序编程接口（API）实施数据交互，遵循“业务必需、最小权限”原则，对接口设计、开发、服务及运行等环节实施集中安全管控。

When engaging third-party institutions for data collaboration, The Bank developed the *Data Security Management Measures*, according to which, we strictly isolate internal and external

risks when collaborating with third-party institutions for data collaboration, exchange data through centrally managed external engagement platforms or application programming interfaces (APIs) under the principles of "business necessity and minimum access", and implement comprehensive security controls across all stages, including interface design, development, service, and operations.

与第三方机构共同处理数据时，遵循"业务必要授权"原则制定技术方案，通过合同协议明确双方数据安全责任与义务，并采取有效管理和技术保护措施确保数据安全。

When processing data with third-party institutions, the Bank develops technical solutions based on the principle of "authorization based on business needs", clearly defines both parties' data security responsibilities and obligations through contractual agreements, and takes effective management and technical protection measures to ensure data security throughout the process.

委托第三方处理个人客户信息时，合同条款明确受托方的保护义务、措施及期限，严格监督其按约定目的和方式处理数据，传输客户个人敏感信息前须通过加密、脱敏等技术确保安全，防范滥用与泄露风险，且未经授权不得转委托。

When engaging a third party to process customers' personal information, the Bank ensures that the engaged party's obligations, protection measures, and processing duration are explicitly defined in contractual terms. The Bank strictly supervises the third party's processing of data according to the agreed purpose and method. Before transmitting sensitive customer information, the third party shall ensure data security through encryption, anonymization, or other technical means to prevent misuse or leakage. Delegation of data processing without the Bank's authorization is prohibited.

本行制定《中国农业银行业务外包管理办法》，规范包括独立第三方以及本行设立在境内外的子公司、关联公司或附属机构等在内的服务商的外包行为，明确要求服务商充分保障本行客户信息安全。（财务会计部）在科技外包活动的服务实施阶段，持续进行全流程监控，通过建立信息资产授权清单、开展外包人员信息安全培训、开展网络安全评估及数据安全检查等措施，严格落实外包服务安全管理要求。

The Bank formulated the *Administrative Measures on Business Outsourcing of Agricultural Bank of China* to standardize the outsourcing activities of service providers, including independent third parties and domestic and overseas subsidiaries, affiliates or subsidiaries established by the Bank, with specific requirements that service providers shall fully guarantee the information security of the Bank's customers. During the service implementation stage of technology outsourcing activities, the Bank continuously conducts end-to-end monitoring, strictly implements security management requirements for outsourcing services through measures such as establishing an authorization list for information assets, conducting information security training for outsourcing personnel, and carrying out cybersecurity assessments and data security inspections.

建立第三方机构数据处理异常监测机制，持续强化内外部人员监督管理。

The Bank established a monitoring mechanism for abnormal data processing activities by third-party institutions, and continued to strengthen supervision and management of both internal and external personnel.

除法定情形或已依法获取授权外不对外提供客户信息

Prohibiting the Disclosure of Customer Information to External Parties except under Legal Circumstances or Duly Authorized

本行通过隐私政策向客户承诺：除法律、行政法规有明确规定的情形，如订立、履行客户作为一方当事人的合同所必需，或履行本行法定义务所必需等，本行不会对本行以外的公司、组织和个人提供客户的个人信息。如因业务需要确需对外提供客户个人信息的，本行会在提供前向客户告知个人信息接收方的相关信息、处理目的、处理方式和个人信息的种类等，依法获得客户单独同意或授权，法律法规另有规定的除外。

The Bank promises customers through its privacy policy that, except in cases explicitly stipulated by laws and administrative regulations, such as when necessary for the conclusion and performance of contracts involving customers as a party, or for the fulfillment of the Bank's legal obligations, the Bank shall not provide customers' personal information to companies, organizations, or individuals outside the Bank. If there is an actual business need to provide customers' personal information externally, the Bank shall inform customers of information about the recipient of their personal information, purposes and means of processing, and types of personal information, and obtain separate consent or authorization from customers in accordance with the law, unless otherwise stipulated by laws and regulations.

加强文化建设与培训

Strengthening Cultural Development and Training

本行高度重视员工在信息安全、隐私数据保护及商业秘密保密等方面的培训教育工作，建立面向全体员工、劳务派遣用工和外包人员等第三方人员的多维度、系统化、专业化的培训体系。

The Bank places great emphasis on training and education in areas such as information security, privacy data protection, and the confidentiality of trade secrets, and established a multi-dimensional, systematic, and professional training system that covers all employees and third-party personnel, such as labor dispatch workers and contractors.

数据安全培训。本行致力于培育良好的数据安全文化，坚持将数据安全要求融入日常业务管理。一是以农银 e 学为学习渠道，面向全集团员工开展数据安全教育和培训，建立数据安全知识学习专栏，发布数据安全管理、数据安全管理实践等课程，系统介绍数据安全系统性、普及性介绍、本行管理实践中需要全体员工关注的重点工作等，同时通过楼宇视频滚动播放、办公终端弹窗安全提示等方式全方位强化数据安全意识，全面提升员工的数据安全保护意识与技能水平，营造全员共同维护数据安全、助推业务发展的良好氛围。二是面向总分行数据安全管理人员组织开展专业能力培训，通过专题培训、交流研讨，系统普及“管什么、在哪管、怎么管”的数据安全管理实施路径，制作并传导了委外催收、开放银行、联合建模等 5 个重点场景数据安全管理规范视频，有力提升了数据安全管理人员的业务能力。

Data security training. The Bank is committed to fostering a strong culture of data security by integrating data security into business management. First, the Bank organizes data security education and training programs for all employees of the Group through ABC E-Learning under a dedicated section for data security knowledge, offering courses on data security management and data security management practice. The courses include a systematic and comprehensive overview of data security, as well as priorities that require the attention of all employees. In addition, the Bank reinforces data security awareness through various means, such as rolling video displays in office buildings and pop-up security alerts on office terminals to comprehensively enhance employees' awareness and capabilities in data protection, and to foster a culture in which everyone contributes to data security and business development. Second, the Bank organizes professional training sessions targeting data security managers at the Head Office and branches. Through specialized training sessions and discussions, the Bank systematically promotes the implementation path of data security by clarifying the scope, area, and methodology of data security management. Additionally, video training materials on data security management standards are prepared and distributed, focusing on five key scenarios, including outsourced collection, open banking, and joint modeling. These efforts have significantly enhanced the professional capabilities of data security management personnel.

个人信息保护培训。本行重点提升基层一线及法律、消保等专业岗位人员在客户个人信息保护领域的履职能力。编制《个人信息保护法标准培训课件》，系统梳理司法判例、监管处罚案例，围绕告知同意、机构合作、人工智能等易引发法律纠纷的重点难点领域。组织个人信息保护"滴灌式"培训，开设"月月谈"空中课堂，发布"每周一案"。

Personal information protection training. The Bank focused on improving the performance capabilities of frontline staff and those in legal, consumer protection, and other professional roles to protect customer personal information. We compiled the *Standard Training Materials on the Personal Information Protection Law*, which includes a systematic analysis of relevant judicial precedents and regulatory enforcement cases, focusing on key and complex areas that are prone to legal disputes, such as notice and consent, institutional cooperation, and the application of artificial intelligence. The Bank also organized micro training sessions on protection of personal information, "Monthly Insights" online learning courses, and published "Case of the Week" publication.

劳务派遣用工及外包人员等第三方人员培训。将劳务派遣用工、外包人员等第三方人员纳入数据安全培训范围，明确违规责任、提升安全意识。培训内容涵盖《数据安全管理办法》基础规范、外包业务数据安全管理要求等。报告期内，通过与第三方合同、协议明确外包服务供应商数据安全培训具体要求条款，按照"谁使用谁负责"的原则由行内相关机构组织对外包服务人员开展培训。

Training for labor dispatch workers, contractors and other third-party personnel. These personnel are included into data security training programs to clarify accountability for violations and enhance data security awareness. The training program covers basic standards in the *Data Security Management Measures* and data security requirements for outsourced operations. During the reporting period, the Bank specified data security training requirements for outsourcing service providers through contractual terms and agreements. Relevant bank departments organized training sessions for outsourced personnel in accordance with the principle that "the person who uses data shall also bear the corresponding responsibility" to ensure compliance with data security obligations.

本行将数据安全风险纳入全面风险管理体系，相关风险情况纳入全面风险管理报告。建立分工负责、协调联动的数据安全风险监测机制，对数据安全威胁实施有效监测，开展监督检查，主动评估风险，防范数据篡改、破坏、泄露及非法利用等安全事件发生。

The Bank incorporated data security into its comprehensive risk management system, and included relevant risk profile into the comprehensive risk management report. Specifically, the Bank established a risk monitoring mechanism for data security underpinned by clear division of responsibilities and coordination, to effectively monitor data security threats, conduct inspections and supervision, proactively assess risks, and prevent security incidents such as data tampering, destruction, leakage, and illegal use.

加强应对数据安全事件能力

Enhancing Capabilities to Respond to Data Security Incidents

构建全覆盖的数据安全应急响应体系。本行制定《中国农业银行数据安全事件应急预案》，明确事件分类定级标准、报告与处置流程、职责分工及责任追究机制；确保一旦发生数据安全事件，能够迅速成立应急团队，采取有效措施控制风险蔓延，及时减轻事件造成的危害与不利影响。

Building a comprehensive data security emergency response system. The Bank formulated the *Data Security Incident Emergency Response Plan of Agricultural Bank of China* to define incident classification and grading standards, reporting and disposal procedures, division of labor, and accountability mechanisms. The document ensures that in the event of a data security incident,

the Bank could quickly establish an emergency response team, take effective measures to control risks, and mitigate the hazards and adverse impact in a timely manner.

- **事前预防 Proactive risk prevention**

风险监测：在全行超 40 万台办公终端部署终端数据防泄露系统（终端 DLP）；持续开展敏感数据整治工作；制定《办公终端数据安全管理工作指引》，建立常态化管控机制；推进系统用户行为数据分析挖掘项目，建立用户权限与异常行为的风险预警规则，构建数据系统用户数据安全风险监测模型。

Risk monitoring: We deployed terminal data breach prevention systems (DLP) on over 0.4 million office terminals across the Bank and continued to conduct rectification over sensitive data; formulated the *Guidelines for Data Security Management of Office Terminals* and established a routine management mechanism. Meanwhile, we advanced the user behavior analytics project, established risk alert rules for user permissions and abnormal behaviors, and built a monitoring model for users' data security risks.

常态化演练：每年根据最新风险态势制定年度演练方案，组织覆盖总行、境内分行、境外分子行及子公司的全面演练，保障各机构、各部门有效应对数据安全事件与威胁；通过随机通知、不预先公开泄露线索等方式，模拟真实场景对分支机构开展压力测试，以战带训，切实检验并提升应急响应能力。

Regular drills: Each year, the Bank develops an annual drill plan based on the latest risk landscape, and organizes comprehensive drills that involve the Head Office, domestic branches,

overseas branches, subsidiary banks, and subsidiaries. These drills ensure that all institutions and departments are well-prepared to respond to data security incidents and threats. Furthermore, by simulating real-world scenarios, the Bank conducts stress tests over affiliates randomly and without prior disclosure of specific clues. By doing so, the Bank evaluates and improves its ability to respond to emergencies.

- 事后管控

- **Post-event control**

本行成立数据安全事件应急处置领导小组，明确数据部门、科技部门、消费者权益保护部门等在内的常务成员。一旦发生数据被篡改、泄露、破坏、非法获取、非法利用等数据安全事件，能够迅速成立应急团队，立刻启动应急处置机制，采取有效措施控制风险蔓延，及时减轻事件造成的危害与不利影响，同时按照合同、协议等有关约定履行客户及合作方告知义务。

The Bank established a leading group for emergency response to data security incidents, with clearly defined standing members including the data department, IT department, and consumer protection department. In the event of a data security incident, such as tampering, leakage, damage, illegal acquisition or misuse of data, the Bank could quickly establish an emergency response team to activate the emergency response mechanism immediately, take effective measures to contain the spread of risks, promptly mitigate the hazards and adverse impact in a timely manner. Moreover, the Bank fulfills its obligations to inform customers and partners in accordance with relevant contracts or agreements.

建立业务连续性容灾体系

Establishing a Business Continuity and Disaster Recovery System

本行建立面向业务连续性的容灾体系，主要业务全部实现灾备、重要业务全部实现全链路双活，37 家分行人工网点全部实现 4G 灾备网络建设。常态化组织开展分行联合容灾切换演练，增强实战演练的覆盖面和实战性。

The Bank established a reactive system for business continuity, with all major businesses backed up, and all key operations supported by full-chain active-active architecture. All manual outlets of 37 branches developed 4G disaster recovery networks. Joint disaster recovery switchover drills were organized on a routine basis in branches to enhance the coverage and practical effectiveness of practical drills. The information systems remained stable under the sustained high-performance operations.

完善专项审计

Improving Special Audits

本行高度关注数据安全审计，每年至少实施一次相关内部审计项目。通过网络信息安全管理审计、网络与数据安全管理审计、数据治理审计等 IT 审计项目，覆盖数据安全相关内容，重点关注数据安全治理、外部合作数据安全、行内数据安全、应急管理等方面。

The Bank places significant emphasis on data security audits and conducts at least one relevant internal audit project annually. Through IT audit initiatives such as audits of network information

security management, network and data security management, and data governance, the Bank ensures comprehensive coverage of data security-related areas. Key focus areas include data security governance, data security in external collaborations, internal data security practices, and emergency response management.

外部审计机构（第三方会计师事务所）每年对本行信息科技治理体系和管理体系开展全面审计与评估，重点涵盖信息科技发展规划、信息科技风险管理、信息安全管理、信息系统开发测试管理、信息系统运行管理、信息科技外包管理、业务连续性管理等。外部审计对象包括境内分行，总行业务相关部门、科技相关部门、风险管理相关部门。审计时遵循的准则和标准包括《商业银行信息科技风险管理指引》、《银行业金融机构全面风险管理指引》、《银行保险机构数据安全管理办法》、《银行保险机构信息科技外包风险监管办法》、《商业银行业务连续性监管指引》等现行有效的监管规定。

Each year, an external audit firm (a third-party accounting firm) conducts a comprehensive audit and evaluation of the Bank's information technology governance and management systems. This includes key areas such as IT strategic planning, IT risk management, information security, system development and testing management, IT operations management, IT outsourcing management, and business continuity management. The external audits cover domestic branches, relevant business departments at the Head Office, technology departments, and risk management departments. The audit process adheres to standards including the *Guidelines for Information Technology Risk Management in Commercial Banks*, *Guidelines for Comprehensive Risk Management in Banking Institutions*, *Administrative Measures for Data Security in Banking and Insurance Institutions*, *Regulatory Measures for Information Technology Outsourcing Risks in*

Banking and Insurance Institutions, and *Regulatory Guidelines for Business Continuity in Commercial Banks*, and other currently effective regulatory requirements.

2025 年，本行未发生重大数据安全事件、泄露客户隐私事件和网络安全事件。

In 2025, the Bank did not experience any major data security incidents, breaches of customer privacy, or cybersecurity incidents.

本行明确数据安全管理的中长期目标，贯彻落实国家和行业数据安全监管要求，建立与本行业务发展相适应的数据安全治理体系，坚持维护国家安全和本行利益，保护消费者合法权益，统筹数据安全和数据应用，保障数据的正常合理使用。

The Bank has established medium- and long-term goals for data security management, implemented national and industry data security regulatory requirements, and built a data security governance system that was aligned with the Bank's business development to safeguard national security and the Bank's interests, protect the legitimate rights and interests of consumers, and coordinate data security with data application to ensure the proper and reasonable use of data.

一是建立健全数据安全治理架构，形成牵头部门抓统筹、条线机构抓落实、“三道防线（业务、风险、审计）”抓监督以及业技融合、协同推进的工作合力。强化全员数据安全意识，将数据安全纳入日常风险管理，构建人人参与、齐抓共管的数据安全大格局。

First, we establish and strengthen the data security governance structure to foster synergies where leading departments take charge of overall planning, business line units implement measures, the “three lines of defense (business, risk, and audit)” ensure oversight, and business and technology

functions work in an integrated and collaborative manner to jointly advance data security work. Meanwhile, we enhance data security awareness of all employees, incorporate data security into daily risk management, and build a data security framework featuring collective responsibility and joint management.

二是聚焦敏感级及以上数据、个人信息等重点数据，紧盯数据出行、信息系统、办公终端、开发测试、邮件外发、业务外包等重点场景和事项，强化数据安全保护措施落实，严防数据批量泄露风险。

Second, we focus on key data categories, including sensitive data and above, and personal information; closely monitor important scenarios and activities such as data export, information systems, office terminals, development and testing, external email communication, and business outsourcing; strengthen the implementation of data protection measures to prevent the risk of mass data breaches.

三是坚持维护数据安全与促进数据开发利用并重，严格按照法规制度和标准规范开展数据安全保护，保障数据广泛深入应用。

Third, we place equal emphasis on data protection and the promotion of data utilization, strictly follow laws, regulations, and standards in implementing data protection measures, thus enabling secure and extensive application of data.