隐私和数据安全进展

Progress on Privacy and Data Security

一、 应对数据泄露的措施

I. Measures to Address Data Breaches

1.加强应对数据安全事件能力

1.Enhancing Capabilities to Respond to Data Security Incidents

本行构建集团全覆盖的数据安全应急管理机制，持续完善数据安全事件应急处置流程。全行层面，制定《中国农业银行数据安全事件应急预案》作为数据安全事件的总体预案，提出了数据安全事件的监测、报告、处置与演练的总体要求。执行层面，各部门、各分支机构在总体预案基础上，针对主管业务、系统和场景制定场景级预案，明确了各场景的应急处置流程和标准。

We have established a group-wide comprehensive data security emergency management mechanism and continues to refine the response procedures for data security incidents. At the bank-wide level, *the Data Security Incident Emergency Response Plan of Agricultural Bank of China* has been formulated as the overarching plan for data security incidents, setting forth overall requirements for monitoring, reporting, handling, and drills of such incidents. At the execution level, each department and branches developed scenario-specific contingency plans based on the overarching plan, tailored to their respective business areas, systems, and scenarios, thereby clarifying the emergency response procedures and standards for each scenario.

- **事前预防**
- **Proactive measures**

本行高度重视日常的应急演练，聚焦频发和易发风险，遵循“真演真练”原则，常态化开展场景演练、压力测试、攻防拉练三类演练。数据安全场景演练，以真实情境切入，业务主管、消保、舆情、科技、法务各类角色各负其责，不断增强跨部门、跨机构层级应急处置的配合程度；数据安全压力测试，采取不预设场景、不提前通知、不区分机构层级的方式，将数据泄露线索分发至应急处置机构，要求迅速排查和处置，验证应急处置能力特别是报告的及时性；网络和数据安全联合拉练，在攻防实战中发现漏洞短板，在检验应急响应能力的同时，探查潜在安全漏点。

We attach great importance to daily emergency drills, focusing on frequent and easily occurring risks. Adhering to the principle of “real drills for real practice”, it regularly conducts three types of exercises: scenario-based drills, stress tests, and offensive-defense training. Data security scenario drills are conducted by entering real-world situations, where business executives, consumer protection officers, public opinion specialists, technology personnel, and legal counsel each assume their respective responsibilities to continuously enhance cross-departmental and cross-institutional coordination in emergency response. Data security stress tests are performed without predefined scenarios, advance notice, or distinction of institutional levels; data breach leads are distributed to emergency response agencies, requiring immediate investigation and disposal to verify emergency response capabilities, particularly the

timeliness of reporting. Joint network and data security exercises are carried out to identify vulnerabilities and weaknesses through offensive and defensive combat operations, simultaneously testing emergency response capabilities and probing for potential security loopholes.

- 事中监测
- In-process Monitoring

本行持续开展外部情报和内部线索的风险监测，对各类异常情况和事件风险做到早报告、早处理，形成数据安全态势感知能力。外部方面，依托行业联防联控机制，将监管机构发布的共享情报、信息通报、风险提示、行业预警等外部数据安全威胁情报纳入风险监测，及时发现、识别数据安全风险，并基于网络与数据安全联防联控和监管机构态势感知机制，及时报告数据安全事件风险线索。对内方面，本行建立数据安全监测平台，对数据对外提供、信息系统等风险场景开展多渠道、多节点的监测和预警。数据对外提供场景已实现互联网通道的涉敏监测，建立运行态和管理端的闭环管理机制；信息系统场景通过大模型工具智能识别异常操作行为线索，积累监测规则并形成预警基线库。

We continue to conduct risk monitoring based on external intelligence and internal leads, ensuring early reporting and early handling of various abnormal situations and event risks, thereby establishing data security situational awareness capabilities. Externally, relying on the industry-wide joint prevention and control mechanism, external data security threat intelligence issued by regulatory authorities, including shared intelligence, information notifications, risk warnings,

and industry alerts, is incorporated into risk monitoring to timely identify and detect data security risks. Furthermore, based on the network and data security joint prevention and control framework and the regulatory authority's situational awareness mechanism, clues regarding data security incident risks are reported in a timely manner. Internally, the Bank has established a data security monitoring platform to conduct multi-channel and multi-node monitoring and early warning for risk scenarios involving external data provision and information systems. Monitoring of sensitive data exposure scenarios via internet channels has been implemented, establishing a closed-loop management mechanism for runtime and management interfaces. In information system scenarios, large model tools are utilized to intelligently identify clues of abnormal operational behaviors, accumulating monitoring rules to form a warning baseline library.

- **事后管控**
- **Reactive measures**

本行未发生过数据安全事件，如发生或发现数据安全事件，本行将按照应急预案，快速高效完成信息报告，准确评估数据损失情况，立即开展应急处置。数据安全事件发生或发现后，事发机构需选取最有效便捷的方式，及时报告至总行数据安全事件应急处置领导小组（设置在本行管理层），对符合监管报告情形的，应满足 2 小时向行业主管部门报告，24 小时内提交书面报告等要求，涉及特别重大的事件，还应按照规定及时向属地公安部门报告，重点报告事件基本情况、受影响的数据敏感程度和数据量级等数据损失情况等，并按照法

律法规或合同协议约定，及时履行客户及合作方告知义务。同时，迅速开展应急处置，深入分析事件原因，采取措施遏制影响，阻断风险扩大，有效控制事态，进一步降低负面影响。数据安全事件处置结束后，本行事发机构应总结处置情况，开展根因分析，完善相关制度，优化相关系统，在30日内形成书面报告。如发生个人客户信息泄露、毁损、篡改、丢失等事件，根据合同、协议有关约定和我行应急管理制度相关规定，我行将及时采取有效补救措施，阻止安全事件扩大。事件相关情况将及时告知个人客户（法律、行政法规另有规定不通知的除外），告知方式包括电子邮件、信函、电话和/或推送通知等；难以逐一告知时，我行会采取合理、有效的方式发布公告。告知内容包括发生或者可能发生泄露、毁损、篡改、丢失的个人信息种类、原因和可能造成的危害；我行已采取和将要采取的补救措施；个人可以采取的减轻危害的措施；我行个人信息保护负责人的联系方式等。

No data security incidents occurred at the Bank. Should any data security incident occur or be discovered, the Bank will promptly and efficiently complete information reporting in accordance with its emergency plan, accurately assess the extent of data loss, and immediately initiate emergency response measures. Upon the occurrence or discovery of a data security incident, the institution involved shall promptly report the matter to the leading task force for emergency response to data security incidents at the Head Office (established under the senior management of the Bank) via the most effective and convenient means available. For incidents that meet regulatory reporting requirements, reports must be submitted to the relevant industry

regulatory authority within two hours, followed by a written report within 24 hours. In cases involving particularly major incidents, the local public security authorities must also be notified in a timely manner in accordance with applicable regulations. The report shall focus on the basic circumstances of the incident, the sensitivity level of the affected data, the volume of data involved, and other details regarding data loss. Furthermore, the obligation to notify customers and partners shall be fulfilled promptly in compliance with applicable laws, regulations, or contractual agreements. Simultaneously, emergency response measures were promptly initiated, the root causes of the incident were thoroughly analyzed, and actions were taken to contain the impact, prevent the expansion of risks, effectively control the situation, and further mitigate negative consequences. Upon conclusion of the data security incident response, the institution involved in the incident shall summarize the response measures, conduct a root cause analysis, improve relevant policies, and optimize related systems, and prepare a written report within 30 days. In the event of a data security incident, such as breach, destruction, alteration, or loss of personal customer information, we will promptly implement effective remedial measures according to the relevant terms of applicable contracts and agreements, as well as our internal incident response policies, to prevent the security incident from escalating. Affected customers will be promptly notified of the incident details, unless otherwise exempted by applicable laws or administrative regulations. Notifications will be delivered via email, postal mail,

telephone, and/or push notifications. Where individual notification is impracticable, we will issue a public announcement through reasonable and effective means. The notification will include: the categories, causes, and potential adverse impacts of the personal information that has been or may be subject to breach, destruction, alteration, or loss; remedial measures already implemented and those to be undertaken; recommended actions individuals can take to mitigate potential harm; and contact information for our Personal Information Protection Officer.

二、 隐私增强技术与举措

II.Privacy enhancing technologies and initiatives

1.信息系统数据全生命周期安全保护。

1.Full-lifecycle Data Security Protection for Information Systems.

本行通过《中国农业银行数据安全管理办法》，明确了信息系统数据全生命周期保护的总体要求，并专门制定了《中国农业银行信息系统数据全生命周期保护规范》，针对数据收集、存储、使用、加工、传输、提供、销毁的全生命周期，提出了兼顾业务管理和技术保护的一体化要求。

We have established the *Data Security Management Measures of Agricultural Bank of China* to clarify the general requirements for the protection of data throughout the entire lifecycle of information systems. Additionally, we have specifically formulated the *Information System Data Lifecycle Protection Standards of Agricultural Bank of China*, which proposes integrated requirements balancing business management and

technical protection covering the entire data lifecycle, including collection, storage, use, processing, transmission, provision, and destruction.

本行正式发布了重点信息系统和重点数据处理活动清单。针对重点信息系统，对照《中国农业银行信息系统数据全生命周期保护规范》开展评估，并对评估发现的问题，制定完善方案并实施安全加固。针对重点数据处理活动，通过《中国农业银行重点数据处理活动安全管理工作指引》提出了“原则性禁止+例外统一规范管理”的要求，并完成了重点系统的例外评估，完善了补偿保护措施。面向本行全量信息系统的数据处理活动，着力提升事前需求评估的工具化自动化，通过大模型智能识别敏感数据处理活动，自动填写数据安全需求，为项目实施、上线监控提供了事前依据。

We have officially published the list of key information systems and key data processing activities. For key information systems, an assessment was conducted in accordance with the *Information System Data Lifecycle Protection Standards of Agricultural Bank of China* and comprehensive remediation plans were formulated and implemented to address security vulnerabilities identified during the assessment. For key data processing activities, the *Guidelines for Security Management of Key Data Processing Activities of Agricultural Bank of China* stipulated requirements of “principle-based prohibition plus unified standardized management of exceptions,” completed exception assessments for key systems, and enhanced compensatory protection measures. To support data processing activities across the Bank's entire information system,

initiatives have been implemented to improve the automation and tooling of pre-project requirements assessments. By leveraging large models for intelligent identification of sensitive data processing activities, data security requirements are automatically populated, providing a basis prior to project implementation and go-live monitoring.

三、 员工隐私和数据安全培训范围

III.Scope of Employee Training on Privacy and Data Security

1.加强文化建设与培训

1.Strengthening Cultural Development and Training

本行高度重视员工在数据安全、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。

We place great emphasis on training and education in areas such as data 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。依托全员考试、专项培训班、线上视频课、案例手册、现场指导等方式开展培训，内容涵盖数据安全法律法规、行业标准和监管制度、数据安全案例、数据分类分级、安全管理要求和技术保护要求、第三方合作中的数据安全保护、数据安全事件应急处置等。2025 年，全行开展数据安全培训 500 余场次，覆盖

超 40 万境内外员工。

Data security training. We are committed to fostering a strong culture of data security by integrating the requirements for data security into routine business management. Training was conducted through various methods, including comprehensive examinations, specialized training sessions, online video courses, case study manuals, and on-site guidance. The content covered data security laws and regulations, industry standards and regulatory policies, data security cases, data classification and grading, security management requirements and technical protection requirements, data security protection in third-party collaborations, and emergency response to data security incidents. In 2025, over 500 data security training sessions were organized, covering more than 0.4 million employees.

我行高度重视培训师资力量，多层级开展数据安全培训，邀请监管机构、同业标杆、本行管理层、各部门和各级机构的主要负责人和数据安全专家，面向员工开展培训。我行高度重视培训受众覆盖度，多对象开展数据安全培训，受众涵盖全集团的专兼职员工及三方合作对象，对不同受众开展差异化培训：面向管理层，主要授课内容为数据安全风险案例；面向重点领域业务部门，介绍重点业务场景管控措施；面向分支机构，讲解数据安全工作内容和数据安全实施路径；面向涉及外包的业务部门，强调三方合作中的数据安全要求；面向境外机构，介绍数据安全管理思路和境外重点场景管控落实。

We place high importance on training faculty and conducted data security training at multiple levels. We have invited key personnel from

regulatory authorities, peer benchmarks, our Bank's management, principal responsible person of various departments and institutions at all levels, as well as data security experts to deliver training to employees. The Bank places high importance on the coverage of training audiences and conducts data security training for multiple groups. The audience encompasses full-time and part-time employees across the entire Group as well as third-party partners. Differentiated training was delivered to distinct audiences: for management, the primary content focused on data security risk cases; for business departments in key areas, control measures for key business scenarios were introduced; for branches, the scope of data security work and implementation pathways were explained; for business departments involving outsourcing, data security requirements in third-party cooperation were emphasized; and for overseas institutions, data security management concepts and the implementation of controls for key overseas scenarios were presented.

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《中国农业银行数据安全管理办法》、外包业务数据安全管理要求、个人信息保护、三方合作中的数据安全要求等，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，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。2025 年，总分行面向劳务派遣用工开展了外部审计、开发测试等类型的数据安全培训，覆盖 1.5 万人次，面向外包人员等第三方人员开展数据合作相关的 53 类重点场景的培训，覆盖 12

万人次参加。

Training for labor dispatch workers, contractors and other third-party personnel. Labor dispatch workers, contractors and other third-party personnel were included into data security training programs to clarify accountability for violations and enhance data security awareness. The training program covered the *Data Security Management Measures of Agricultural Bank of China*, data security requirements for outsourced operations, personal information protection, and data security requirements in third-party cooperation. In accordance with the principle of "whoever uses is responsible," relevant internal institutions organized training for outsourced service personnel, while specific clauses regarding data security training requirements for outsourced service suppliers were clearly stipulated through contracts and agreements with third parties. In 2025, the head office and branch offices conducted external audits and development testing data security training for labor dispatch employees, covering 15,000 person-times. Additionally, training on 53 key scenarios related to data cooperation was provided to third-party personnel, including outsourced staff, with 120,000 participants.

四、数据保护措施覆盖供应商和商业伙伴

IV.Data Protection Programs Covering Suppliers and Business Partners

1.第三方数据及隐私安全管理

1.Third-Party Data and Privacy Security Management

- 加强从第三方获取数据的安全管理
- Strengthen the security management of data obtained from third parties

本行制定《中国农业银行外部资讯服务管理办法》，建立并实施了外部数据采购和合作引入的集中审批机制。为强化外部数据引入的安全管控，发布了《中国农业银行外部数据服务管理工作指引》，对需求收集、安全评估、数据接入、运维管理、登记备案、风险管控和监督评价建立了闭环管理机制，并将外部数据采购与合作纳入外包风险管理体系。本行以项目为抓手强化数据安全的全流程管控，事前开展项目评估，重点核查来源合规性、个人客户授权同意情况、数据提供者的安全保障能力和潜在风险，并通过协议明确数据安全责任；事中持续监控，确保协议合同条款以及安全保护措施得到具体落实；事后监督评价，对成效不达预期或存在隐患的项目予以退出。本行建设了总分行一体化的外部数据平台，支持各类型、格式、体量数据的“参数化”接入，以及运行质量监测和定价计费的“配置化”管理，为全行50余个应用提供了外部数据支撑。

We formulated the *Administrative Measures for External Information Services of Agricultural Bank of China,* established and implemented a centralized approval mechanism for the procurement of external data and the introduction of cooperation. To strengthen the security control of external data introduction, the *External Data Service Management Guidelines of Agricultural Bank of China* was issued. A closed-loop management mechanism has been established for

requirement collection, security assessment, data access, operations and maintenance management, registration and filing, risk control, and supervision and evaluation. Additionally, external data procurement and cooperation have been incorporated into the outsourcing risk management system. The Bank strengthens full-process data security control by taking projects as the focal point. Prior to project initiation, assessments are conducted with a focus on verifying source compliance, obtaining personal customer authorization and consent, evaluating the data provider's security assurance capabilities and potential risks, and defining data security responsibilities through agreements. During project execution, continuous monitoring is performed to ensure that contractual terms and security protection measures are effectively implemented. Post-project, supervisory evaluations are carried out, and projects yielding results below expectations or harboring hidden risks are subject to exit. The Bank has established an integrated external data platform for its head office and branches. This platform supports the 'parameterized' ingestion of data across various types, formats, and volumes, as well as the configurable management of operational quality monitoring and pricing/fee calculation. It provides external data support for more than 50 applications across the entire bank.

- 严禁出租、出售本行数据。
- **Strictly prohibiting the renting, or selling the Bank's data.**

本行严格遵守法律法规和相关监管要求，对业务过程中知悉的数据予以保密，采取管理或技术等有效措施加强对数据的保护，依法使

用工作中获取的数据，不得以任何形式向本行以外的其他机构或个人出租、出售本行数据。

The Bank strictly complies with laws, regulations, and relevant regulatory requirements, keeps confidential customer information obtained in the course of business, takes effective management or technical measures to strengthen data protection, and uses data obtained in the course of work in accordance with the law. Under no circumstances shall the Bank's data be rented or sold to any other institution or individual other than the Bank.

- **严格管理向第三方提供的数据**
- **Strict management of the data provided to third parties**

本行通过《中国农业银行数据安全管理办法》，提出了面向所有第三方机构开展数据合作中的数据主体同意、最小化原则、合同协议约束、履约监督等数据安全管理要求。针对数据合作中所有向第三方提供数据的场景，制定《中国农业银行数据出行安全管理工作指引》，明确数据安全评估、审查审批的机制流程，要求开展风险分析和制定保护措施。

Through the *Data Security Management Measures of Agricultural Bank of China*, we have established data security management requirements for all third-party institutions engaging in data cooperation, including data subject consent, the principle of minimization, contractual constraints, and performance supervision. For all scenarios involving the provision of data to third parties in data cooperation, the *Guidelines for Data Export Security Management of Agricultural Bank of China* have

been formulated, which clarifies the process of data security assessment, review and approval mechanism, and requires the conduct of risk analysis and the formulation of protective measures.

针对委外制卡、委外诉讼、智慧场景等三方合作重点业务场景，制定操作层面的工作规范，针对不同场景定制最小化提供数据的范围，统一合同协议的数据安全条款，细化针对性的保护措施。向第三方提供数据涉及敏感数据和个人客户信息的，执行数据安全评估、审查，第三方合作的项目进行清单制管理，进入清单的，基于数据安全监测平台，设置预警处置机制。

For key third-party cooperation business scenarios such as outsourced card production, outsourced litigation, and smart scenarios, operational work specifications shall be established. The scope of data provision shall be customized to the minimum required for each scenario, data security clauses in contracts and agreements shall be unified, and targeted protective measures shall be detailed. Where the provision of data to third parties involves sensitive data or personal customer information, a data security assessment and review shall be conducted. Third-party cooperation projects shall be managed via a list system; for those included in the list, warning and disposal mechanisms shall be established based on the data security monitoring platform.

全行建立了数据安全监测平台，对三方数据合作开展监测管控，将互联网通道纳入运行态监测范围，以应用程序接口为粒度识别行内向第三方机构提供的数据内容及涉敏情况，设立预警规则，发现三方数据合作实际数据流出时的风险并及时处置。

We have established a data security monitoring platform to monitor and control third-party data collaborations. Internet channels have been incorporated into the runtime monitoring scope. Data content provided by the Bank to third-party institutions and sensitive information involved are identified at the granularity of application programming interfaces. Warning rules have been established to detect risks associated with actual data outflows during third-party data collaborations and to enable timely disposal.

- **第三方数据合作的数据安全风险排查**
- **Data security risk investigation regarding third-party data cooperation**

本行重视三方数据合作的风险排查，每年定期通过现场和非现场结合的方式，开展重点风险线索的评估排查，并推动高风险问题的整改提升。本行重点排查委外制卡、委外诉讼等数据委托处理，联合建模等数据共同处理，以及本行数据托管或存储在行外第三方等情形，覆盖我行与第三方数据合作项目的事前、事中、事后全流程数据安全管控情况。事前重点围绕数据处理活动的必要可行性、潜在风险和配套安全保护措施、数据合作清单管理等；事中关注数据安全风险监测发现的问题；事后聚焦履约监督情况。对排查出的风险隐患，结合业务特点和风险特征制定整改措施，形成排查整改工作台账，从同类问题整合、制度机制优化、技防管控强化、第三方数据交互模式集中化管理等方面做好完善提升。

We place high importance on risk screening for third-party data cooperation. Annually, it conducts assessments and screenings of key risk clues through a combination of on-site and off-site methods and promotes

the rectification and improvement of high-risk issues. The Bank conducted a focused investigation into scenarios involving data entrusted processing, such as outsourced card issuance and outsourced litigation, joint data processing, such as collaborative modeling, and data custody or storage with third parties outside the Bank. This review assessed data security controls throughout the entire lifecycle of the Bank's third-party data collaboration projects, covering pre-engagement, active engagement, and post-engagement phases. Prior to the activity, focus is placed on the necessity and feasibility of data processing activities, potential risks and supporting security protection measures, and management of the data cooperation list; during the activity, attention is given to issues identified through monitoring of data security risks; and after the activity, emphasis is placed on the supervision of contract fulfillment. For identified risks and hidden dangers, rectification measures shall be formulated in light of business characteristics and risk features. A ledger for inspection and rectification work shall be established to ensure comprehensive improvement through the integration of similar issues, optimization of policies and mechanisms, strengthening of technical prevention and control, and centralized management of third-party data interaction models.