中国国际金融股份有限公司数据安全及隐私保护政策声明

Policy Statement of Data Security and Privacy Protection of China International Capital Corporation Limited

中国国际金融股份有限公司（以下简称“中金公司”或“公司”）秉承“植根中国，融通世界”的理念，致力于为多元化的客户群体提供高质量金融增值服务，目标是打造成为具有国际竞争力的一流投资银行。

China International Capital Corporation Limited (“CICC” or the “Company”) is committed to the mission of “Chinese roots and international reach”, and strives to provide high-quality, value-added financial services to a diversified client base, with the goal of becoming a first-class investment bank with international competitiveness.

公司在数字化变革的加速演进中，高度重视数据安全和隐私保护治理，严格遵循《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《网络数据安全管理条例》《信息安全技术 个人信息安全规范》《证券基金经营机构信息技术管理办法》《证券期货业网络和信息安全管理办法》《证券期货业数据安全管理与保护指引》《证券期货业数据分类分级指引》《证券期货业移动互联网应用程序安全规范》《个人金融信息保护技术

规范》等法律法规及监管要求，持续推进公司数据安全与隐私保护体系建设工作，强化网络和信息安全防护能力，保障个人信息主体权益。

Amid the accelerating evolution of digital transformation, the Company places high importance on the governance of data security and privacy protection, strictly complying with applicable laws and regulations including *Cybersecurity Law of the People's Republic of China*, *Data Security Law of the People's Republic of China*, *Personal Information Protection Law of the People's Republic of China*, *Regulations on Network Data Security Management*, *Information Security Technology—Personal Information Security Specification*, *Administrative Measures for Information Technology of Securities Investment Fund Institutions*, *Administrative Measures for Network and Information Security in the Securities and Futures Industry*, *Guidelines for Data Security Management and Protection in the Securities and Futures Industry*, *Guidelines for Data Classification and Grading in the Securities and Futures Industry*, *Security Specifications for Mobile Internet Applications in the Securities and Futures Industry*, and *Technical Specification for Protection of Personal Financial Information*. The Company continuously advances its data security and privacy protection framework while strengthening network and information security safeguards to protect the rights of personal information subjects.

一、管理架构

I. Management Structure

公司建立了完善的数据安全管理架构，以保障公司数据安全，具体包括：数据安全决策组织、数据安全管理组织、数据安全执行组织。

The Company has established a comprehensive data security management framework to safeguard corporate data security, which specifically includes Data Security Decision-Making Body, Data Security Management Body, and Data Security Execution Body.

表 中金公司数据安全管理架构

Table: CICC Data Security Management Framework

层级 Level	职责 Responsibilities
数据安全决策组织 Data Security Decision-Making Body	信息技术治理委员会是公司数据安全决策组织，由负责信息技术工作的公司领导班子（管委会）成员担任主席，首席信息官担任执行主席。负责对公司数据安全相关工作的重大事项进行审议和决策，监督数据安全相关工作的开展。 The IT Governance Committee is the data security decision-making body of the Company. The committee is chaired by a member of the Company's Management Committee overseeing IT, with the CIO as Executive

层级 **Level**	职责 **Responsibilities**
	Chair. The IT Governance Committee is responsible for reviewing and making decisions on major issues pertaining to the Company's data security initiatives, while also exercising supervisory oversight to ensure the effective execution of data security-related operations.
数据安全管理组织 Data Security Management Body	信息技术部作为公司数据安全管理组织，负责牵头公司的数据安全管理工作。 The IT Department is the data security management body of the Company, and is responsible for the overall data security management efforts of the Company.
数据安全执行组织 Data Security Execution Body	公司各部门为数据安全执行组织，负责将数据安全相关要求纳入本部门制度中，推动数据安全管理规范在部门内部的落实。 All departments are execution bodies of data security, and are responsible for integrating data security requirements into departmental policies and promoting the execution of data security management protocols within the department.

二、管理制度

II. Management System

公司持续推进数据安全制度体系建设，制定了《中国国际金融股份有限公司数据安全管理实施细则》《中国国际金融股份有限公司数据分类分级管理指引》《中国国际金融股份有限公司数据权限管理指引》《中国国际金融股份有限公司数据生命周期管理指引》《中国国际金融股份有限公司数据脱敏管理指引》等管理制度，该等制度适用于公司各部门、公司实际控制的境内外子公司和分支机构，主要规范数据全生命周期的安全管理，以明确公司数据安全的基本要求与管控措施。

The Company continuously advances its data security regulatory framework through formally established policies including *China International Capital Corporation Limited Data Security Management Implementation Rules*, *China International Capital Corporation Limited Data Classification and Grading Management Guidelines*, *China International Capital Corporation Limited Data Access Rights Management Guidelines*, *China International Capital Corporation Limited Data Lifecycle Management Guidelines*, and *China International Capital Corporation Limited Data Desensitization Management Guidelines*. These foundational documents apply uniformly to all Company departments, domestic and overseas subsidiaries, and branch offices effectively controlled by CICC. They primarily

standardize the security management throughout the entire data lifecycle, aiming to clarify the fundamental requirements and control measures for the Company's data security.

公司主要的线上对客服务 APP 已公开其隐私政策并明确告知客户，包括《中金金禾隐私政策》《中金股票 APP 隐私协议》《中金研究院服务平台隐私政策》《中金火炬隐私政策》《中金资本荟隐私政策》《中金固收 APP 隐私政策》《"中金点睛"数字化投研平台隐私政策》《中金领易 TradeLink 小程序隐私政策》、中金点睛日文站隐私政策、中金点睛国际站、美国站隐私政策。

The Company's primary online client-facing applications maintain publicly accessible privacy policies with explicit client notifications, including *CICC JINHE Privacy Policy*, *CICC Stock App Privacy Agreement*, *CICC Research Institute Service Platform Privacy Policy*, *CICC Torch Privacy Policy*, *CICC Capital Club Privacy Policy*, *CICC FICC (Fixed Income, Currencies & Commodities) App Privacy Policy*, *CICC Insights Digital Investment Research Platform Privacy Policy*, *CICC Link TradeLink Mini-Program Privacy Policy*, along with privacy policies for the CICC Insights Japanese Site, CICC Insights International Site, and CICC Insights U.S. Site.

三、数据安全主要管理措施

III. Primary Data Security Management Measures

（一） 主被动相结合的数据安全保护措施

A. Integrated Proactive and Reactive Data Security Protection Measures

1. 通过主动措施夯实安全保护基础

1. Establishing Security Foundations through Proactive Measures

公司建立网络和信息安全防护体系，贯彻“安全第一、预防为主；主动防御、综合防范”的方针，实施多层防护，综合采取网络隔离、用户认证、访问控制、策略管理、数据加密、网络防篡改、病毒木马防范、非法入侵检测和网络安全态势感知等安全保障措施，提升网络和信息安全防护能力，及时识别、阻断相关网络攻击。

The Company has established a cybersecurity and information security protection system based on the principle of “Security First, Prevention Foremost; Proactive Defense, Comprehensive Safeguarding.” This multi-layered framework implements security measures including network segmentation, user authentication, access control, policy management, data encryption, tamper-proof network mechanisms, virus/Trojan prevention, intrusion detection systems, and network security posture awareness—collectively enhancing cybersecurity capabilities to promptly identify and block network attacks.

公司制定全方位安全管控措施，包括但不限于人员安全管理、数据安全管理、访问控制管理、密码安全管理、物理环境安全管理、硬件设备安全管理、网络安全管理、系统安全管理、配置管理、日志管理与时钟同步、威胁情报管理、恶意软件控制、终端安全管理、外部安全管理、应急管理、安全符合性、安全检查与评估、网络安全等级保护等。

Comprehensive security controls are implemented across all domains of the Company, including but not limited to: personnel security management, data security management, access control management, cryptographic security management, physical environment security management, hardware device security management, network security management, system security management, configuration management, log management with clock synchronization, threat intelligence management, malware control, endpoint security management, external security management, emergency management, security compliance, security inspection/assessment, and network security classification protection.

2. 通过被动措施做好应急响应、保障及处置

2. Executing Reactive Measures for Emergency Handling and Assurance

公司建立应急管理组织架构，确定重要业务及其恢复目标，制定应急预案，并积极开展应急演练和信息技术应急管理的评估与改进。建立告警应急小组，及时反馈告警信息，

协调组织人员进行研判及应急处置工作。

The Company has established an emergency management organizational structure, identified critical business functions and their recovery objectives, developed contingency plans, and actively carried out emergency drills as well as the evaluation and improvement of information technology emergency management. An alert response team has been set up to promptly report alarm information, coordinate and organize personnel for analysis, judgment, and emergency response efforts.

公司制定并持续完善信息技术应急预案，包括：应急管理建设目标、备份信息系统建设和恢复机制、备份数据恢复机制、业务恢复或替代措施、应急联系方式、与客户沟通方式、向监管部门及有关单位的报告路径、应急预案披露与更新机制等内容。公司根据应急预案定期组织关键岗位人员开展信息技术应急演练。

The Company systematically develops and continuously enhances information technology contingency plans encompassing emergency management objectives, backup system construction and recovery mechanisms, data restoration protocols, business continuity or alternative measures, emergency contact procedures, client communication channels, reporting pathways to regulators and relevant entities, along with disclosure and update mechanisms for contingency plans. The Company regularly conducts IT emergency drills for key personnel in

accordance with its contingency plans.

公司建立信息技术应急处置机制，建立网络安全事件的分级响应机制，明确内部处置工作流程，及时处置网络安全事件，尽快恢复信息系统正常运行，保护事件现场和相关证据，同时按照监管有关规定进行应急报告；发生网络安全事件且对客户造成影响的，及时通过官方网站、客户交易终端、电话或者邮件等有效渠道通知相关方可以采取的替代方式或者应急措施，提示相关方防范和应对可能出现的风险。

The Company has established an information technology emergency response mechanism and a graded response system for cybersecurity incidents. Internal handling procedures have been clearly defined to ensure timely incident containment and swift restoration of normal information system operations. Incident scenes and relevant evidence are preserved in accordance with regulatory requirements, while emergency reporting is carried out as stipulated by supervisory provisions. In the event that a cybersecurity incident has affected clients, the Company shall promptly notify affected parties through effective channels such as its official website, trading terminals, phone calls, or emails, informing them of available alternative methods or contingency measures, and alerting them to potential risks to facilitate prevention and response.

（二） 数据访问控制与保护

B. Data Access Control and Protection

公司建立了数据安全制度规范，实施安全技术措施，防止客户个人信息遭到未经授权的访问、修改，避免数据的泄露、篡改、丢失。

The Company has established comprehensive data security protocols and implemented technical safeguards to prevent unauthorized access or modification of client personal information, thereby mitigating risks of data leakage, tampering, or loss.

公司根据数据重要性与敏感度对数据进行分类分级，并对重要性和敏感度高的数据处理采取严格管控，建立区分敏感数据与非敏感数据的授权审批流程并定期审计。数据访问控制遵循“最少功能、最小权限”原则，根据被授权人工作职责及业务开展的实际需求，仅授予其完成工作所需的最少功能、最小权限。技术层面采用双因素认证，在网络层部署入侵检测系统、入侵防御系统、防火墙等措施，有效进行访问控制管理。

The Company classifies and tiers data according to its importance and sensitivity, imposing stringent controls on the processing of highly critical and sensitive data. It has established differentiated authorization and approval procedures for sensitive versus non-sensitive data, with regular audits conducted to ensure compliance. Data access control follows the principles of “least

functionality and minimum privilege," granting employees only the minimal permissions necessary to perform their job duties and meet actual business requirements. Technically, the Company implements two-factor authentication and deploys network-level security measures—including intrusion detection systems, intrusion prevention systems, and firewalls—to effectively enforce access control management.

公司建立了完整的数据脱敏工作制度和流程保障，实现生产环境到测试环境脱敏工作线上化统一管控；在使用敏感数据时，采用掩码屏蔽等方式进行脱敏，并采取有效措施防范未经授权的拷贝，进行全过程数据使用审计。此外，公司落地了数据安全管控平台和数据脱敏平台，通过数据加密、数据脱敏、去标识化、日志留痕、数字水印等技术手段，加强数据安全防护。

The Company has established a comprehensive data desensitization framework and process governance system, enabling centralized online management of desensitization activities from production to testing environments. When handling sensitive data, masking and other anonymization techniques are applied to protect information, accompanied by strict measures to prevent unauthorized copying and end-to-end auditing of data usage. Furthermore, the Company has implemented a data security control platform and a dedicated data desensitization platform. These systems leverage technical

measures such as data encryption, desensitization, de-identification, operation logging, and digital watermarking to strengthen overall data security protection.

（三） 员工及外包人员管理与培训

C. Employee and Outsourced Personnel Management and Training

公司重视数据安全与隐私保护的培训与考核管理，覆盖全体人员，包括正式员工和外包人员。

The Company prioritizes training and assessment management for data security and privacy protection, comprehensively covering all personnel including full-time employees and outsourced staff.

公司不定期组织员工参加数据安全基础专项培训，同时提供网络安全、信息安全等安全类培训课程，通过培训及宣贯，提高员工的网络和信息安全意识。

The Company regularly organizes specialized training sessions on data security fundamentals for its employees, while also offering additional courses in cybersecurity and information security to enhance employees' awareness in network and information security.

公司外包人员入场时，均会按照相关法律法规、监管要求及公司规定签署“九条底线”及工作承诺书，并参加入场前培训，培训内容涵盖网络和信息安全相关领域。在使用外包服务过程中，以“必需知道”和“最小授权”为原则，为外包人

员申请与其岗位职责相匹配的最小必要权限，同时跟踪监督外包人员落实保密协议的情况。

All outsourced personnel are required to sign the “Nine Bottom Lines” commitment and a work agreement in accordance with relevant laws, regulations, supervisory requirements, and company policies before onboarding. They must also participate in pre-entry training, which covers topics related to network and information security. Throughout the engagement, the Company adheres to the principles of “need-to-know” and “minimum privilege” by granting outsourced staff only the minimum necessary access rights relevant to their roles. Additionally, the Company monitors and supervises the implementation of confidentiality agreements by these personnel.

（四） 供应商安全管理

D. Supplier Security Management

公司积极推动供应商数据安全管理，在采购合同中明确要求供应商对合作过程中知悉的业务信息、文件、资料、数据、客户或者其他非公开信息严格保密，对于信息技术类供应商，要求保证其所提供的软件或技术服务符合关于网络安全、数据安全、个人信息安全的法律法规，符合国家及证券期货业网络和信息安全相关的技术管理规定、技术规则、技术指引和技术标准。

The Company actively promotes data security management among its suppliers. Procurement contracts explicitly require

suppliers to maintain strict confidentiality of any business information, documents, materials, data, customer details, or other non-public information obtained during collaboration. For information technology suppliers, additional obligations are imposed to ensure that all provided software or technical services comply with laws and regulations concerning cybersecurity, data security, and personal information protection, as well as adhere to national and securities and futures industry-specific technical management regulations, technical rules, guidelines, and standards related to network and information security.

（五） 认证及防线

E. Certifications and Defense Mechanisms

中金公司通过 ISO27001 信息安全管理体系认证，覆盖中金公司信息技术部提供信息系统开发、测试、运维服务的100%业务。每年定期开展体系内审，并接受发证机构的监督外审。

CICC maintains ISO 27001 Information Security Management System certification, covering 100% of the business operations within its IT Department, including system development, testing, and maintenance. Annual internal audits are conducted alongside external surveillance audits by certification bodies.

公司高度重视数据管理与数据安全工作，通过了数据管理能力成熟度评估模型三级（DCMM）、数据安全建设能力

认证（DSCC），并在此基础上持续深化数据治理与数据安全体系建设，持续完善数据安全管理制度与流程。

The Company prioritizes data management and security, and has achieved Level 3 certification under the Data Management Capability Maturity Assessment Model (DCMM) and obtained the Data Security Construction Capability (DSCC) certification. Building upon these, CICC continuously enhances data governance frameworks , while consistently refining data security policies and procedures.

公司建立信息科技 1.5 道防线管理体系，形成信息科技风险事前、事中、事后全链路风险管理。公司定期针对重点领域开展专项风险评估，主动识别、排查信息技术风险点，建立完善信息科技风险相关制度，加强信息科技风险识别、评估、处置、跟踪、监控全生命周期管理。

The Company has established a 1.5-line defense management system for information technology, enabling end-to-end risk management covering pre-event, in-process, and post-event phases. It conducts regular specialized risk assessments in key areas to proactively identify and address IT risk exposures. The Company has developed and continues to refine comprehensive information technology risk management policies, strengthening the full lifecycle management of IT risks—including identification, assessment, mitigation, tracking, and monitoring.

公司根据《企业内部控制基本规范》及其配套指引的规定和其他内部控制监管要求、《证券基金经营机构信息技术管理办法》《中国国际金融股份有限公司信息技术内部审计工作指引》等内外部规定，聘请有资质的会计师事务所每年开展内部控制审计并涵盖信息技术有关内容，定期开展信息技术外部专项审计，以及定期开展信息技术内部审计工作，涵盖信息技术安全管理等领域。公司通过审计揭示问题“上半篇文章”和做好审计整改“下半篇文章”，持续推动相关领域信息技术管理提升。

In compliance with *Basic Standards for Enterprise Internal Control* and its supporting guidelines, other regulatory requirements on internal control, internal and external regulations including *Administrative Measures for Information Technology of Securities Investment Fund Institutions*, and *Information Technology Internal Audit Guidelines of China International Capital Corporation Limited*, the Company has hired qualified accounting firms to conduct annual internal control audits, which include coverage of information technology-related areas. It also carries out regular external specialized IT audits and internal IT audits covering fields such as information technology security management. Through these audits, the Company focuses on both revealing issues (the “first half” of the audit process) and implementing corrective actions (the “second half” of the audit process), thereby continuously improving the management of

information technology in relevant domains.

四、客户隐私保护管理措施

IV. Customer Privacy Protection Management Measures

公司严格遵守《中华人民共和国个人信息保护法》《信息安全技术 个人信息安全规范》等法律法规及标准，在各对客产品隐私政策中，明确了业务开展各个环节中处理客户信息的管理规范，以保障客户个人信息安全。

The Company strictly complies with laws, regulations, and standards such as the *Personal Information Protection Law of the People's Republic of China* and the *Information Security Technology—Personal Information Security Specification*. In the privacy policies of all customer-facing products, the Company clearly defines management protocols for handling customer information at every stage of business operations to ensure the security of customers' personal data.

（一）客户个人信息的处理

A. Processing of Customer Personal Information

公司基于"权责一致、目的明确、选择同意、最少够用、确保安全、主体参与、公开透明"原则，按照公司各产品和服务发布的隐私政策中明确声明和告知的目的、方式和范围，收集和使用客户个人信息，不超范围收集和使用客户个人信息，不收集提供服务非必要的客户个人信息。

The Company collects and uses customers' personal information in strict accordance with the principles of

“Alignment of Authority and Responsibility, Purpose Specification, Informed Consent, Minimum Necessary, Ensured Security, Stakeholder Engagement, and Openness and Transparency.” All processing activities are conducted within the purpose, methods, and scope explicitly stated and communicated in the privacy policies of the Company’s various products and services. The Company does not collect or use personal information beyond the declared scope, nor does it gather any personal data unnecessary for the provision of its services.

公司对客户的个人信息进行严格保密。在确需对外提供客户个人信息时，公司会充分评估对外提供的合法性、正当性、必要性，并且严格遵守相关法律法规、监管要求或协议约定保障客户个人信息安全。若涉及委托处理个人信息的场景，公司会与受托方根据法律规定签署相关处理协议，明确约定双方的权利和义务，并对受托方的个人信息处理活动进行监督。若涉及共同处理个人信息的场景，公司会与合作方根据法律规定签署相关协议并约定各自的权利和义务，确保在处理相关个人信息的过程中遵守法律法规的相关规定。

The Company maintains strict confidentiality of customers’ personal information. In circumstances where it is necessary to provide such information to external parties, the Company shall conduct thorough assessments to ensure the legality, legitimacy, and necessity of such actions, and strictly comply with applicable laws, regulations, regulatory requirements, and contractual

agreements to safeguard the security of customers' personal information. In scenarios involving entrusted processing of personal information, the Company shall sign legally compliant data processing agreements with entrusted parties, clearly defining the rights and obligations of each party, and monitor the personal information handling activities of these entrusted entities to ensure compliance. In cases of joint processing of personal information, the Company shall enter into agreements with partners in accordance with legal provisions, specifying respective rights and responsibilities, to ensure that all parties involved adhere to relevant laws and regulations throughout the processing of personal data.

公司按照法律法规、监管规定、公司内部规定及合同协议等法定或约定的方式和保存期限对客户个人信息进行存储，超出前述保存期限的个人信息，公司将在合理期限内依照所适用的法律对所持有的客户个人信息进行删除或匿名化处理。

The Company stores customers' personal information in accordance with the methods and retention periods stipulated by laws, regulations, regulatory requirements, internal company policies, and contractual agreements. For any personal information that exceeds the aforementioned retention period, the Company shall, within a reasonable timeframe and in compliance with applicable laws, delete or anonymize the retained customer

personal information.

（二）赋予客户的权利

B. Customer Rights Empowerment

公司重视客户对个人信息的管理，并尽全力保障客户对其个人信息的查阅、复制、修改、删除、撤回同意授权等权利，以使客户有能力保障其隐私安全。

The Company values its customers' ability to manage their personal information and makes every effort to safeguard their rights to access, copy, modify, delete, and withdraw consent for their personal data, thereby empowering them to protect their privacy and security.

客户可以通过专门渠道查询、更正注册的个人信息；公司仅在为客户提供服务所必需的期限内和适用法律规定的时限内留存客户个人信息，如客户个人信息超出法律法规、监管规定、公司内部规定及合同协议等法定或约定的保存期限或发生政策声明的特定场景时，公司将进行删除或匿名化处理；客户可通过隐私政策约定的联系方式联络公司改变同意范围或撤回授权，撤回授权后公司将不再收集相关的个人信息。

Customers may inquire about and correct their registered personal information through designated channels. The Company retains personal information only for the period necessary to provide services to customers and within the time limits stipulated by applicable laws. If the retention of customer

personal information exceeds the statutory or agreed storage periods specified by laws, regulations, regulatory requirements, internal company policies, or contractual agreements, or if specific scenarios outlined in policy statements occur, the Company will delete or anonymize such information. Customers may contact the Company through the contact methods specified in the privacy policy to modify the scope of consent or withdraw authorization. Upon withdrawal of authorization, the Company will cease collecting the relevant personal information.

此外，公司提供隐私政策的访问渠道、个人信息权利行使指引，并提供热线、邮箱等方式供客户随时联系。客户相关权利的详细说明，可参考公司各产品和服务发布的隐私政策。

The Company provides accessible channels for reviewing its privacy policies, guidelines on exercising personal information rights, and multiple contact methods such as hotlines and email addresses for customers to reach out at any time. For detailed information regarding relevant rights, customers may refer to the privacy policies published for the Company's various products and services.

（三）产品和服务开发规范

C. Product and Service Development Standards

公司在产品和服务开发过程中，通过及时更新隐私政策、制定相关信息安全制度规范并实施安全技术措施，保障客户

个人信息安全。具体措施如采用去标识化技术脱敏、传输层安全协议、数据隔离技术、数据分级权限管理等，尽力确保个人信息安全。

The Company ensures the security of customers' personal information throughout the development of its products and services by promptly updating privacy policies, establishing relevant information security regulations, and implementing technical safeguards. Specific measures include the use of de-identification techniques for data desensitization, Transport Layer Security (TLS) protocols, data isolation technologies, and data classification-based access control, all aimed at rigorously protecting personal information.