Statement of Haitong Securities Co., Ltd. on Information Security and Customer Privacy Protection Management

As a large state-owned financial enterprise group, Haitong Securities Co., Ltd. (hereinafter referred to as Haitong Securities or the Company) has always paid great attention to information security and customer privacy protection. The Company has established a strict management mechanism covering the full lifecycle of data flow and every link of business operation in a bid to safeguard information security and customer privacy in all respects.

I. Management Mechanism

Haitong Securities has attached great importance to information security and customer privacy protection. It has strictly abode by national laws, regulatory provisions and industry regulations on information security including the *Data Security Law of the People's Republic of China*, the *Personal Information Protection Law of the People's Republic of China*, the *Regulations of the People's Republic of China on the Security Protection of Computer Information Systems*, etc. and regulated the management of customer information and transaction data, to ensure information security and transaction security of all customers.

i. Management structure

The Company has refined the information security and data governance structure and responsibility assignment mechanism and established a top-down information security and customer privacy protection management structure with clearly defined responsibilities. The information security and customer privacy protection management structure comprises the decision-making level, the management level, the execution level and the supervision level. The decision-making level is composed of the IT Governance Committee and the leading group for network and information security which administer the Company's personal information protection work and network and information security work respectively. The IT Governance Committee has set up the Data Governance Office, whose daily office institution is in the Operating Center and performs the functions of coordinating and managing the personal information protection work of the Company. The leading group for network and information security has set up the office of the leading group for network and information security, whose daily office institution is in the Data Center. Co-led by Chairman and General Manager, the leading group for network and information security ensures effective implementation of personal information protection work.

Information Security and Privacy Protection Management Structure of Haitong Securities

Level	Department/committee	Responsibilities
Decision-making level	Leading group for network and information security	• Sets up the office of the leading group for network and information security, makes overall planning for the network and information security work of the Company, and organizes, coordinates and advances relevant efforts;

		• Chairman and General Manager co-lead the leading group for network and information security.
	IT Governance Committee	• Performs decision-making functions concerning the personal information protection of the Company; • Deliberates on the Company's data governance objectives, work plans and implementation of plans.
Management level	Office of the leading group for network and information security	• Its daily office institution is in the FinTech Department. The office of the leading group for network and information security is headed by the person in charge of the Data Center; • Responsible for promoting and implementing the company's network security management and ensuring its day-to-day operation.
	Data Governance Office	• Performs coordination and management functions concerning the personal information protection of the Company; • Promotes, executes and puts in place data governance related work of the Company; • The daily office institution of the Data Governance Office is in the Operating Center. The director of the Data Governance Office is the person in charge of the Operating Center.
Execution level	Taskforce for personal information protection	• Executes the personal information protection work of the Company. It is composed of Operating Center, FinTech Department, Digital Finance Department, Wealth Management Headquarters, Securities Finance Department, Private Banking Department, Corporate Finance Department, Software Development Center, Data Center, Compliance Management Department, Risk Management Department, etc.; • Organizes preparation of personal information protection management policies and regulations, establishes the organizational structure and management mechanism for personal information protection, develops

		personal information protection solutions and organizes their implementation; • Organizes personal information protection related training to gradually enhance the capability of specialized personnel and the safety protection awareness of employees; • Oversees and inspects the personal information protection by the Company and subsidiaries, circulates problems, and urges them to make remediation; • Establishes and refines the personal information protection evaluation mechanism.
Supervision level	Audit Department	• As the supervisory department of personal information protection work; • Periodically audits the Company's compliance with laws, administrative regulations and the Company's management regulations when handling personal information; • Issues audit reports, urges the Company to remedy problems, and ensures effective implementation of personal information protection work.

ii. Management regulations

According to the *Personal Information Protection Law of the People's Republic of China*, the *Information Technology Management Measures of Securities and Fund Operators*, the *Technical Specification of Protection of Personal Financial Information* and other relevant laws and regulations, the Company has formulated and constantly updated and revised privacy protection management policies and regulations, including the *Management Measures of Haitong Securities Co., Ltd. for Personal Information and Privacy Security Protection*, the *Management Measures of Haitong Securities Co., Ltd. for Customer Information* and the *Privacy Protection Policy of e-HaitongCai APP*, as well as information and data security management policies and regulations such as the *Management Measures of Haitong Securities Co., Ltd. for Data Classification and Grading*, the *Measures of Haitong Securities Co., Ltd. for Information Security Management*, the *Information Assets Security Management Measures of Haitong Securities Co., Ltd.* and the *Implementation Rules of Haitong Securities Co., Ltd. on Security Management of Storage Media of Production Systems*. The policies are applicable to all business lines of the Company, and subsidiaries may use them as reference based on local laws and regulations and the regulatory requirements of corresponding industry.

Type	Policy name
Privacy protection	*Management Measures of Haitong Securities Co., Ltd. for Personal Information and Privacy Security Protection*
	Management Measures of Haitong Securities Co., Ltd. for Customer Information
	Privacy Protection Policy of e-HaitongCai APP
Information security	*Measures of Haitong Securities Co., Ltd. for Information Security Management*
	Management Measures of Haitong Securities Co., Ltd. for Network System Security
	Management Measures of Haitong Securities Co., Ltd. for Data Classification and Grading
	Information Assets Security Management Measures of Haitong Securities Co., Ltd.
	Implementation Rules of Haitong Securities Co., Ltd. on Security Management of Storage Media of Production Systems

II. Information Security Management

Haitong Securities attaches great importance to information security management. Following the policy of "clear responsibilities, reasonable authorization, standard procedures and combination of technology and management" and the requirements of the *Data Security Law of the People's Republic of China*, the *Personal Information Protection Law of the People's Republic of China*, etc., the Company has formulated a number of policies including the *Management Measures of Haitong Securities Co., Ltd. for Information Security*, the *Management Measures of Haitong Securities Co., Ltd. for Network System Security* and the *Management Measures of Haitong Securities Co., Ltd. for Personal Information and Privacy Security Protection*, standardized the management of all customer information and transaction data, regularly and irregularly conducted internal and external information security inspections, implemented information security protection measures to effectively ensure the information security and transaction security of all customers. Based on regulatory requirements and the Company's internal management regulations, at least one internal audit and one external audit on data security and privacy protection are conducted every year. The Company had no customer information leakage in 2022.

i. Information security protection measures

In terms of information security protection mechanism, the Company has established an all-round protection system that includes proactive preventive measures and passive countermeasures.

1. Proactive preventive measures

- The Company has established a vertical-horizontal defense system (four lines of defense and four key areas) and it conducts real-time monitoring 24/7 and responds via the security operation platform. It conducts correlation analysis of logs from different devices and multi-source intelligence. It has designed multi-associated scenarios to support real-time detection, real-time

grading and classification and real-time warning of the security operation center. It enriches warning information to discover threats like cyberattacks, viral transmission, loopholes in a timely manner so that front-line monitoring personnel can deal with all security incidents in a timely and closed-loop manner.

- The Company's securities operation platform automatically orchestrates fixed response procedures and effectively blocks malicious IP through SOAR (Security Orchestration, Automation and Response), thus jamming attacks.
- The Company performs routine effectiveness validation of cybersecurity protection measures in cooperation with the BAS (Breach and Attack Simulation) platform. It validates the effectiveness, anti-bypass security capability and coverage degree of cybersecurity protection devices on both the internet side and the intranet side, constantly upgrades validation scenarios, and optimizes validation effect. The non-customer systems on the internet side use the zero trust technology and make sure that all of those that should be included are included.
- In terms of inter-department collaboration within the Group, the Company set up a "beacon tower" of integrated commands for branches and subsidiaries, realized internal sharing of threat information and collaborative handling, and put in place a whole set of technology self-examination systems and responsibility fulfillment systems covering the headquarters, branches, subsidiaries and service providers.

2. Passive countermeasures

- The Company has formulated the *Contingency Plan of Haitong Securities for Network Security Events*, which covers four scenarios, namely, data leak, data corruption, personal information leak and personal information tampering. The Company updates the contingency plan according to relevant situational changes in a timely manner.
- The Company holds relevant training of the contingency plan, security testing and emergency drills periodically. Through national-level and Company-level cybersecurity attack and defense exercises, the Company constantly validates the effectiveness of protection measures and strengthens the practical capability of the cybersecurity team so it can respond to all types of emergencies at any time. The Data Center conducts two "Red-Blue-Purple" confrontational drills each year, summarizes experience and develops special actions to correct problems found, such as actions to narrow down exposures, fortify passwords and authority and so on. In 2022, Haitong Securities was rated "Excellence" in the national network security drill.

ii. Information security inspection

1. External inspection

In terms of external inspection, the Company conducts external audit based on cybersecurity level protection work and ISO27001 certification requirements and implements audit management of information security governance.

In terms of cybersecurity level protection, the Company performs a cybersecurity level protection evaluation on a yearly basis and makes sure that a plan is developed and implemented and relevant problems are corrected. The Company currently has 10 level protection systems that have been registered and put on record with relevant authority (3 three-level systems and 7 two-level systems). The evaluation of all the systems was completed in 2022. The Company has planned a total of 18 level protection systems in 2023, including 4 three-level systems (including 1 new system) and 14 two-level systems (including 7 new systems).

The Company has obtained the ISO27001 certificate (valid till April 7, 2025), which covers 100% data centers of the Company, of which the main data center is the machine room on Dean Road, Pudong New District and the offsite backup data center is the machine room (SZSE South Center) in Fenggang Town, Dongguan City, Guangdong Province. All the Company's business systems are deployed in the two machine rooms.

On May 9, 2023, Haitong Securities' e-HaitongCai APP obtained the security certificate for mobile internet application programs (both Android and iOS platforms) in securities and futures industries from China Securities Information Technology Services Co., Ltd. The APP security certificate (valid till May 8, 2026) covers all businesses of e-HaitongCai APP from the wealth management business line of Haitong Securities.

Meanwhile, the Company engages a professional third-party institution to audit its IT management work from time to time. At the end of 2021, the Company engaged KPMG to audit its IT management work. KPMG examined the Company's organizational structure for data governance, data classification and grading, data security, authority management, data application and other data governance works.

2. Internal inspection

In terms of internal inspection, according to regulatory requirements and the Company's internal management regulations, the Company carries out a series of information security review activities every year to examine the organizational structure for data governance, data classification and grading, data security, authority management, data application, etc. The Company has launched a special self-inspection campaign, in which business departments comb through customer information protection of systems in their charge and put forth measures for improvement. The campaign aimed at figuring out the situation of customer information protection in business systems. The campaign aims at figuring out the situation of customer information protection in business systems. Meanwhile, the Company inspects IT operation maintenance every quarter and network and information security every year on contents including IT governance, data governance, information security, etc. In November 2022, the Audit Department conducted a special audit on IT governance and inspected data governance related work including data security, data use, data destruction, privacy protection, data backup and data classification.

III. Privacy Protection Management

The Company fully respects and protects user privacy. It has formulated the *Management Measures of Haitong Securities Co., Ltd. for Personal Information and*

Privacy Security Protection and the *Management Measures of Haitong Securities Co., Ltd. for Customer Information*, to standardize the management of user privacy data and information. The e-HaitongCai APP is the main platform where the Company obtains customers' personal information. The Company has formulated the *Privacy Protection Policy of e-HaitongCai APP*, which covers the wealth management business line of the Company and is applicable to all personal users of the e-HaitongCai APP.

i. Information collection and storage

1. Collection

In terms of user information collection, the Company has created a list of personal information for collection and use and a list of personal information for sharing with third parties and required its institutions to only collect the minimum information necessary for business processing. In addition, the Company will not collect personal data from third parties (unless otherwise required by law). Meanwhile, the *Privacy Protection Policy of e-HaitongCai APP* has clearly informed customers of the scope of data collected and the purposes of use of data and fully revealed personal rights, purposes of use of customers' relevant data and other contents.

2. Storage

Haitong Securities will only retain users' personal information for the purposes described in the "E-Haitongcai APP Privacy Policy," for the necessary duration, and within the time limits stipulated by laws, regulations, and regulatory requirements. Article 137 of the Securities Law of the People's Republic of China says that "securities companies shall properly keep customers' account opening materials, trust records, transaction records and information relating to internal management and business operation; no one shall hide, fabricate, tamper with or damage such information; and such information shall not be kept for less than 20 years". Therefore, Haitong Securities has separated background data acquisition from the historical database and retained data with tape library backup till the expiry of the retention period stipulated by law. For registered community member users of e-Haitongcai APP, when they cancel their membership, the Company will delete the data related to them within 15 days (unless otherwise required by law).

ii. Right of control over personal information

When users use the e-HaitongCai APP, the Company provides users with various services including but not limited to access, change or modification, withdrawal of consent, account cancellation, refusal of personalized push, autonomous management, personal information protection, etc. to ensure users' right of control over personal information.

1. Access

When an individual requests query of his or her information according to law or when an individual requests transfer of his or her information to a designated third party and that meets the conditions specified by the national department of cyberspace affairs, the Company will promptly provide access or transfer paths.

2. Modification

The users could modify their information via various channels including online and offline (counter, witness, etc.). Users of the e-HaitongCai APP may inquire and modify their personal data on the "business processing" page.

3. Deletion

Users of the e-HaitongCai APP may apply to delete their relevant data as individual community members by canceling their accounts. Moreover, when an individual withdraws the consent of information collection authorization, the Company will delete his or her personal information. If an individual finds that relevant information is not deleted, he or she may request the Company to delete relevant data by calling the customer service hotline 95553 or contacting online customer service representatives.

iii. Access control and protection

1. In terms of access control, according to the *Management Measures of Haitong Securities Co., Ltd. for Personal Information and Privacy Security Protection*, the Company has established the personal information access control management mechanism, which strictly isolates different functional zones through firewall access control. Meanwhile, based on business needs and the least privilege principle, the Company reasonably controls and assigns personal information access and uses policies and operation privileges to make sure that different functional personnel have corresponding level of information access and avoid operations beyond authority.

2. In terms of protection mechanism, according to the *Management Measures of Haitong Securities Co., Ltd. for Personal Information and Privacy Security Protection*, the Company's IT departments ensure safe storage of personal information through such technical means as data encryption, authentication and access control and de-identify and anonymize those that do not require complete display of certificate No., account, name, reserved mobile phone number or other ID information. Meanwhile, the Company implements category-by-category, level-by-level management of personal information, focuses on protection of other personal information, and strictly protects sensitive personal information. The Company has established and refined the category-by-category, level-by-level data management policy and management system, strengthened identification of level of sensitivity of personal information, and implemented corresponding security policies and protection measures.

iv. Privacy protection measures in product development

The Company requires not using real personal information in development and testing environments. If real personal information is needed in testing, the operation maintenance department shall de-identify and anonymize the information before using it. If undesensitized data are used in the development or testing environment, the same level of security control measures for the production environment shall be used. In the development stage of open source technology application, the Company has introduced professional software from the artifacts library, performs dependency management of more than 100,000 open source components, and periodically scans high risk loopholes and open source licenses to promote safe development. In terms of mobile application, the Company has standardized mobile terminal security, identity authentication, network communications security, data security, development security and security audit and met the requirements of the *Security Specifications of Mobile Internet Application Programs in Securities and Futures Industries (JR/T 0192-2020)*.

In May 2023, the e-HaitongCai APP completed the APP security certification for securities and futures industries. In terms of big data application, relevant requirements must be subject to business compliance evaluation.

IV. Capability Building and Partner Management

i. Information security training

To enhance employees' information security protection awareness and risk identification capability, the Company periodically organizes information security education activities, such as National Cybersecurity Awareness Week. Meanwhile, the Company spreads ideas of information security and privacy protection to all employees by pushing knowledge via email, putting up posters, releasing online learning courses, etc. In 2022, the Company held a total of four training sessions on information security awareness and data security management, which had 7,500 participants in total. Besides, in 2022, ten promotional activities were organized to timely popularize the country's laws, regulations and industry standards with respect to data security of personal information, data governance and so on.

ii. Management of IT service providers

The Company's IT service providers mainly include hardware manufacturers, agent hardware service providers, application software manufacturers, agent software service providers, information consulting service providers, information security service providers, data content service providers, HR outsourcing service providers, technical support service providers, basic software manufacturers, telecom operation service providers, etc. According to the *Management Rules of Haitong Securities Co., Ltd. for IT Service Providers*, all IT suppliers shall sign a non-disclosure agreement with the Company and undertake to strictly abide by the requirement of keep data secrecy in the non-disclosure agreement and to not provide personal data to any third party.

In the information system launch, procurement bidding, supplier selection and performance management process, the Company requires the foregoing service providers to earnestly formulate policies and plans on confidentiality, data protection, etc. and it assesses, oversees and tracks project bidding and contract performance.

In the data and information contract templates, the Company has included articles on partners' prohibited acts, articles on partners' commitments on product security and articles on partners' confidentiality commitments and signs a non-disclosure agreement with partners to restrict relevant supplier behaviors.

In terms of relevant compliance check and testing regulations and procedures, the Company's IT service provider management department and compliance risk management department conduct necessary review and evaluation of IT service providers and restrict the access, data use, confidentiality obligations and responsibilities of service providers and service personnel through contract and agreement review, performance acceptance and tracking, etc.

If the Company finds an IT service provider or relevant party violates the regulations on storage or use of the Company's operational data or customer information, the Company will require the IT service provider or relevant party to immediately make correction and destroy the operational data or customer information it has obtained. If the IT service provider or relevant party refuses to make correction, the Company will

immediately stop cooperation and take measures to protect the Company's and its customers' legitimate rights and interests. If the IT service provider is responsible for an information security incident, the Company will suspend or terminate the cooperation with the IT service provider based on the confirmed severity of the case.

According to Article 34 of the *Management Measures of Information Technology of Securities and Fund Operators*, unless otherwise specified by law or the China Securities Regulatory Commission, securities and fund operators shall not provide customer information to any institution or individual in any way. Therefore, the Company will not lease, sell or provide customer information to any third-party institution or individual in any form (unless it is required by law or the CSRC or to complete transaction and provide services).

Meanwhile, according to Article 68 of the *Management Measures of Haitong Securities Co., Ltd. for Data Governance*, the Company shall record the use of operational data and customer information and continuously oversee the implementation of the non-disclosure agreement by relevant parties including IT service providers. In the annual filing of third-party service providers, the Company requires them to provide investor information confidentiality commitment. The Company inspects the annual operation maintenance by stationed personnel and continuously oversees the performance of the non-disclosure agreement. The Company has included IT service providers' protection of investor information and performance of the non-disclosure agreement into its annual evaluation. In its 2022 evaluation, the Company didn't find any leak incident among IT service providers.