

中国工商银行河南分行

电子银行服务的共同条款和条件（202505 版）

第一条 定义

下列术语在本共同条款和条件中解释如下：

1. “电子银行”是指支持客户通过网络和终端设备自行办理和使用自助银行服务的服务。中国工商银行河南分行电子银行通过网上银行、手机银行等为客户提供查询、转账汇款、在线支付结算以及金融管理等资金管理服务。
2. “客户”是指在银行开立账户的个人或组织。
3. “电子密码器”指具有显示屏和数码键盘的可生成动态密码的安全认证设备。
4. “SMS OTP”指客户进行网上银行/手机银行交易时，系统将通过客户已登记的手机号码发送一次性密码。
5. “SOFT TOKEN”（电子保安编码器）/ “DIGITAL TOKEN”指安装在客户手机银行上。客户在网上银行/手机银行进行交易时，将通过手机银行输入 SOFT TOKEN/DIGITAL TOKEN 密码进行交易验签。
6. “人脸识别”/ “生物识别”指通过人脸识别方式进行交易验签。其中，该人脸信息需与客户公民身份证卡或身份证中所加密的人脸信息或银行所采集和检查客户的人脸信息需一致。
7. “安全介质”是指银行用于保护客户交易安全，验证身份的物理或电子设备的工具，包括但不限于 SMS OTP、SOFT TOKEN、DIGITAL TOKEN 或银行当时提供的工具。
8. “电子银行业务指令”指客户通过网上银行/手机银行发出的转账汇款等指令。
9. “自助注册”指已在中国工商银行河南省分行已开通账户的客户通过网银或手机银行自行注册电子银行用户。客户通过自助注册方式开通网银用户可办理查询服务。

第二条 客户的权利、义务

一、权利

1. 客户自愿申请注册银行的电子银行服务，经银行同意后，将有权根据所注册的项目享有相应的服务；
2. 在服务有效期内，客户有权办理注销电子银行的手续；

3. 有权选择注册、变更、关闭验签方式，包括但不限于电子密码器、SMS OTP、SOFT TOKEN、DIGITAL TOKEN、人脸识别以及银行当时提供的验签方式；

4. 客户领取安全介质后，在终止或停止使用电子银行服务时， 无需退还安全介质；对于自助注册用户，无需配套密码器；

5. 若因网络、通讯故障等原因导致客户不能通过电子银行系统办理业务，则客户可到银行营业网点办理业务；

6. 若客户对电子银行服务持有疑问 、 建议或意见 ，可联系热线 18001005（非工作时间）、024.62699818 / 62699830（工作时间）或到银行营业网点进行咨询和投诉。

二、 义务

1. 客户清楚了解使用电子银行服务的过程当中可遭到的风险（包括但不限于信息泄露、信息传递差错、诈骗等），并自愿承担这些风险所导致的任何损失；

2. 客户已经阅读且完全了解本共同条款和条件；

3. 客户确保其用于网上银行/手机银行交易的设备的安全性和可靠性，对于因客户设备故障、通讯故障等原因所导致的经济损失，银行不承担责任；

4. 当领取安全介质时，客户须确认且交回安全介质的领取单，通知银行进行用户激活；

5. 当客户领取安全介质时，应对所有使用安全介质、注册账号（登录 ID）及相应密码的操作负有责任。企业客户必须指定专人妥善保管和使用安全介质、登录信息，不得提供给尚未指定的其他人。同时，应根据客户内部监控的要求合理设置安全介质的操作权限和操作限额，以防范风险、保护账户资金安全；

6. 在客户成功完成指令后，客户不得对支付指令进行变更或撤销；

7. 当客户领取安全介质时，若安全介质在有效期内出现损坏、停用、丢失或出现密码泄露、遗忘等情况，则应及时办理更换、解锁、挂失或密码重置等手续。办理上述手续之前所产生的所有后果由客户承担；

8. 客户在使用电子银行服务的过程中，所提供的资料信息如有更改，客户应及时，主动向银行办理变更手续。办理上述手续之前所产生的一切后果由客户承担；

9. 客户知晓并同意银行采集其人脸信息并用于身份核对、登录手机银行及交易验证等合法用途，客户有义务自行保管好本人的人脸信息，因本人存储等原因导致人脸信息安全事件发生的损失由客户本人承担；

10. 客户应保证已开通电子银行服务的账户的支付能力，并严格执行关于支付结算业务的法律规定。客户需对结算业务的合法与合规承担最终责任，确保符合客户营业许可证（或

其他同等文件)的内容与营业范围内;

11. 客户提交电子银行业务指令时,应保证所提交的指令信息的真实性、完整性和准确性,应明确备注付款用途。客户对支付用途的真实性、合法性负有责任;

12. 如客户发现银行对其通过电子银行服务所提交的指令的处理出现差错,应及时向银行进行通知;

13. 客户使用电子银行服务时,应按照银行关于电子银行业务的相关收费标准进行支付各项费用,并同意让银行主动从其账户扣费;

14. 客户不得以与第三方所发生的纠纷为由来拒绝向银行支付应付款项;

15. 客户不得故意损害银行声誉或恶意攻击银行的电子银行系统;

16. 客户通过电子银行办理业务时,若其所使用的服务功能涉及到银行其他业务规定或规则,则须同时遵守这些业务的规定或规则;

17. 若客户长期不使用电子银行,应主动办理注销手续。

第三条 银行的权利、义务

一、权利

1. 对于因客户泄露用户名、密码、信息或验证方式而导致的任何损失,银行不承担责任;

2. 若客户使用非银行提供的软件、文件或操作指引,由此产生的任何损失银行不承担责任;

3. 银行有权制定电子银行服务的收费标准,并在其正式网站及营业网点进行公布;

4. 银行有权进行电子银行系统的升级、改造;

5. 银行有权自动收集客户下载银行应用的设备信息以检查,审批使用应用、采集生物识别设备并在必要时提供支持跟踪;

6. 为确保客户交易安全,防范风险以及遵守法律规定,银行可有权主动决定每一种验签方式的交易限额;

7. 银行对因客户设备注册、存储他人生物信息而产生的责任予以免责;

8. 在以下情况,银行可单方面主动终止对客户电子银行服务:(i)客户不遵守银行及有关法律规定;(ii)按照政府有关机构要求;(iii)客户存在恶意诋毁和损害银行声誉行为;(iv)银行发现客户存在假冒、诈骗风险;(v)客户尚未按时支付相关费用;(vi)客户属于银行现行《账户使用条款与条件》规定的长期不动户;(vii)自开立电子银行服务起超

过一年而客户未完成安全介质领取手续；

9. 银行根据客户所提交的电子银行业务指令办理业务，为客户办理汇款等业务的时间以电子银行系统中的处理时间为准。对于客户通过电子银行操作的电子信息记录将用于处理电子银行业务的有效依据；

10. 银行因以下情况之一而没有正确执行客户所提交的电子银行业务指令，将不承担任何责任：

- a. 银行收到的指令信息不明确、出错、不完整；
- b. 客户账户余额或授信额度不足；
- c. 客户账户资金被依法冻结或扣账；
- d. 客户未能按照银行相关业务的规定进行正确的操作；
- e. 出现不可抗力或其他非银行原因的情况。

11. 当协议在有效期内终止或停止时，银行不退还客户已缴纳的相关费用；

12. 若因电子银行系统出错、发生故障或其他原因导致客户获得不正当资金，银行有权从客户账户扣划客户所获得的不正当资金或暂停对客户所提供的电子银行服务；

13. 若客户不按照本规定要求的资料提交方式，银行有权拒绝提供电子银行服务给客户。

二、 义务

1. 银行对电子银行所使用的相关软件的合法性负有责任；

2. 银行负责及时为客户办理注册电子银行的手续，并按照客户所注册的功能为客户提供相对应的电子银行服务；

3. 银行负责向客户提供关于电子银行服务的咨询服务，并在银行正式网站上公布业务介绍、解答、交易规则等内容；

4. 银行可在法律许可范围内使用客户的资料和交易明细。银行对客户所提供的文件、资料和信息具有保密的义务，法律另有规定的情况下除外；

5. 当客户登记领取安全介质，且得到银行的接受时，银行须及时将安全介质交给客户；

6. 在银行系统正常运行的情况下，银行负责及时、准确地处理客户所发送的电子银行业务指令并提供如下的服务：

- a. 为客户提供 24 小时的网上账户信息查询服务；
- b. 对于客户所提交的收款人在河内分行开户的支付指令且交易币种为越南盾，银行系统将实时自动处理，并贷记收款人的账户；

c. 对于客户所提交的收款人在越南境内他行开户的支付指令且通过联行系统支付，若客户在工作日 16:00 前提交指令，银行将当日处理，若在工作日 16:00 后提交指令，银行将在下一个工作日内处理；

d. 对于通过自动模块提交的跨境汇款指令，若指令信息准确、完整将于第二个工作日进行处理。客户在提交指令后应主动查询指令状态。

7. 银行可因系统升级、维修而变更或暂停服务，原则上一年不应超过 04 次，累计时间不超过 04 个小时，且银行有责任提前 5 天通知客户有关变更或暂停服务事宜；

8. 当银行收到客户对电子银行服务的反馈时，应及时进行检查并向客户通知检查结果。

第四条 收集和使用客户信息

1. 客户同意与承诺向银行提供准确、真实、齐全的信息。若客户拒绝按照银行要求提供信息，银行可拒绝提供服务；

2. 客户同意银行使用、存储个人信息，或按法律有权机构/个人提供个人信息；

3. 客户接受，同意并允许银行为提高服务质量与客户利益向第三方分享个人信息；

4. 客户同意按银行个人信息保护规定执行本人权利与义务。

第五条 风险提示

1. 若客户同意申请使用银行所提供的电子银行交易服务，客户即被认为已经完全了解电子银行交易的风险，并愿意承担此系统可能带来的损失；

2. 银行采取所有力所能及的有效措施维护客户交易活动和凭证资料的安全性。然而，出于对客户负责任的态度，银行特别提醒客户电子银行服务所存在的风险，包括但不限于：

a. 将银行账户信息、密码或验证码（OTP）存储在手机或浏览器中，且未设置额外安全保护机制，一旦设备被盗或遭非法访问，极易造成账户信息泄露；

b. 下载并安装来源不明的应用程序，或访问含有恶意代码的网站，可能导致设备感染间谍软件，进而导致银行账户信息被窃取；

c. 使用公共网吧访问银行账户，容易遭到黑客监听和数据篡改，造成信息泄露；

d. 若手机操作系统或银行应用程序未及时更新，将无法获得最新的安全补丁，设备可能因漏洞被攻击；

e. 用户可能无意中访问伪装成银行的钓鱼网站或收到诈骗信息（如精心篡改的

URL 链接)，输入个人信息后被不法分子盗取账户资料；

f. 对于企业客户，若内部对业务审批流程管理不严格，允许无授权员工操作交易指令，可能导致财产损失，由客户自行承担；

g. 在极少数情况下，银行系统可能出现处理故障，造成账户余额短暂异常或服务中断。

3. 为确保客户资金安全，银行建议客户：

不以任何形式向任何人提供登录名称、账号、个人信息、密码、OTP 码等；

a. 不安装来源不明的应用程序；

b. 不在公共设备或非安全 Wifi 环境下进行交易；

c. 安装杀毒软件，设置屏幕锁；

d. 仅从 App Store、Google Play、CH Play 的官方渠道或银行提供链接安装应用程序；

e. 若怀疑遭遇诈骗或账户被非法入侵，请立即联系我行，并及时冻结账户，防止资产损失。

第六条 语言

此共同条款和条件以越南文、英文和中文书写。如有冲突，则以越南文版为准。

GENERAL TERMS AND CONDITIONS ON USING E-BANKING

SERVICES OF ICBC HANOI CITY BRANCH

(Version 202505)

Article 1 Definitions

The meaning of the terms used in this General Terms and Conditions is explained as following:

1. “E-banking” is a Banking service that assists The Customer to manipulate automated Banking services by themselves through the internet and terminal equipment. Industrial and Commercial bank of China Hanoi City Branch (“The Bank”) provides the E-banking system via Internet Banking/Mobile Banking to financial management services such as: inquiring account information, remittance, online payment and financial management.

2. “Customer” is an individual, organization opening the accounts at The Bank.

3. “Token Key” is a security device that generates the dynamic codes with a display screen and keyboard.

4. “SMS OTP” is a method in which, when a Customer performs a transaction via Internet Banking or Mobile Banking, the system sends a one-time password (OTP) via SMS to The Customer’s registered phone number.

5. “SOFT TOKEN” / “DIGITAL TOKEN” is a type of authentication method installed in The Customer's Mobile Banking application. When conducting transactions via Internet Banking or Mobile Banking, The Customer enters the SOFT TOKEN / DIGITAL TOKEN code on the Mobile Banking app to authenticate the transaction.

6. “Biometric authentication” / “Facial recognition authentication” / “Face ID authentication” is an authentication method using The Customer’s biometric identifiers that match the biometric data stored in the encrypted information storage unit of the citizen ID card or personal ID card, or the biometric data that has been collected and verified by The Bank.

7. “Security device” is a physical or electronic tool used to verify The Customer, ensuring the security and safety of The Customer’s transactions.

8. “E-banking Instructions” are the inquiry requests of account information, remittance of The Customer which are sent to The Bank via Internet Banking/ Mobile Banking, using Customer

Code (Account number) or security devices and corresponding password.

9. “Online Self-registration” refers to The Customer who has opened an account at the Industrial and Commercial bank of China Hanoi City Branch to self-register E-banking users through online banking or mobile banking. The Customer can apply for inquiry services if they made the Online Self-registration. If The Customer would like to make payment directly, it is required to arrive to The Bank counter to handle it.

Article 2 Rights, obligations of The Customer

1. Rights

- The Customer who voluntarily applies for E-banking services of The Bank, after obtaining The Bank’s written consent, will be entitled to use the corresponding services as registered items;
- During the validity term of the service, The Customer has the right to carry out procedures to terminate the use of E-banking services;
- Customers have the right to choose to register, modify, or cancel authentication methods, including but not limited to Token key, SMS OTP, SOFT TOKEN, DIGITAL TOKEN, biometric authentication, and other authentication methods provided by The Bank from time to time:
- Upon terminating or stopping the services, The Customer is not required to return the security devices; For online self-registered users, no matching Token Key is required;
- Upon occurring the problems such as network or telecommunications errors, The Customer can not perform transactions via The Bank’s E-banking system, The Customer may go to The Bank’s Counter to carry out transactions;
- If there are any questions, suggestions, or feedback about The Bank’s E-banking service, The Customer can contact The Bank via hotline 18001005 (24/7), 024.62699818 / 62699830 (in business time), or go to The Bank’s counter for consultation and guidance.

2. Obligations

- The Customer has fully understood the risks which may be arising in the process of using E-banking services (including but not limited to the risks of information disclosure, documentation mistakes and fraudulent information, etc..) and voluntarily bears all losses caused by these risks by themselves;

- The Customer has read and understood exactly this General Terms and Conditions;
- The Customer must ensure the safety and the reliability of the devices that The Customer uses to carry out transaction via E-banking. The Bank is not responsible of the economic losses caused by The Customer's device trouble and communication problem;
- Upon receiving the security devices, The Customer must confirm and return the receipt of receiving security devices (for Corporate Customer), and request The Bank to activate users;
- Upon receiving the security devices, The Customer is responsible for all actions of using security devices, registration card number (login ID) and related password. The Corporate Customer must designate the responsible person to keep and use the security devices, the login information and should not provide them to the unassigned persons. At the same time, The Customer must base on the internal control requirements of itself to set up the operation rights and the transaction limit reasonably, in order to ensure the account's safety ;
- The Customer is not permitted to change or cancel the payment orders after successfully operating the E-banking transaction instructions;
- If the security devices are damaged, locked, lost or password disclosed, forgotten during the validity term, The Customer should promptly carry out the procedures for changing a new security device, unlocking, claiming of loss, or resetting password. All consequences arising before the completion of the above procedures will be borne by The Customer;
- During the use of E-banking services, The Customer is required to proactively and promptly update their information with The Bank in the event of any changes. Customers shall bear responsibility for any risks that may arise prior to the completion of the relevant change procedures;
- The Customer is responsible for the biometric data registered for logging into Mobile Banking. Customers shall bear liability for any losses arising from their device being used to register or store biometric data of another person;
- The Customer must ensure the solvency of accounts using E-banking service, and strictly abide the relevant legal provisions of payment operations. The Customer is ultimately responsible for the legality and validity of the payment order and ensures that the payment method is complied with the scope and content of operations under the license (or other equivalent legal document);
- Upon performing banking instructions via E-banking, The Customer must ensure the

authenticity, completeness, and accuracy of the transaction information, and must clearly state the purpose of the transaction. The Customer takes responsibilities of the authenticity and legality for the purpose of that payment;

- If The Customer detects any errors in processing transaction instructions via E-banking, The Customer must promptly notify to The Bank;

- Upon using The Bank's E-banking service, The Customer must make payment of fees in accordance with the standard fee schedule issued by The Bank and agrees that The Bank is permitted to proactively collect fees from The Customer's accounts;

- The Customer must not refuse payment of amount owed to The Bank with the reason for a dispute with a third party;

- The Customer must not intentionally damage The Bank's honor or attack The Bank's E-banking system;

- When The Customer performs transaction via E-banking, if the service functions used by The Customer related to other rules or regulations of The Bank, The Customer must simultaneously comply with those rules or regulations;

- If E-banking is not used for a long time, The Customer must proactively apply for termination.

Article 3 Rights, Obligations of The Bank

1. Rights

- The Bank shall not be responsible for any damages arising from The Customer's disclosure of login credentials, passwords, information, or authentication methods for any reason;

- The Bank shall not be held liable in the event The Customer uses software, materials, or follows instructions that are not provided by The Bank;

- The Bank has the right to establish a standard fee schedule for E-banking services and to publish it on The Bank's official website and at its transaction offices;

- The Bank has the rights to upgrade, improve E-banking system;

- The Bank has the right to automatically collect information about the device on which The Customer has installed the application for device identification purposes, to support the assessment and approval of devices registered for login and biometric authentication functions in

accordance with The Bank's regulations, and to assist in monitoring when necessary;

- The Bank proactively decides transaction limits applicable to each type of authentication method to ensure security, minimize risks for customers, and comply with legal regulations;

- The Bank shall be exempt from all liabilities arising from The Customer's device registering or storing biometric data of another person;

- The Bank may unilaterally terminate the provision of E-banking services to The Customer on its own initiative under the following circumstances: (i) The Customer does not comply with The Bank's regulation and relevant legal provisions; (ii) according to the requirements of relevant government agencies; (iii) The Customer maliciously defames and damages the reputation of The Bank; (iv) The Bank found that there was a risk of counterfeiting and fraud; (v) The Customer has not paid the relevant fees on time; (vi) Customers with accounts that have been inactive for a long period as stipulated in The Bank's current "General Terms and Conditions for Account Usage";(vii) One year from the date The Customer registered for E-banking services but has not completed the procedure to receive the security device;

- The Bank shall handle the transactions base on the time and information of The Customer's operations on E-banking;

- If one of the following situations occurs so that The Bank cannot carry out the E-banking order of The Customer exactly, The Bank shall not take any responsibilities:

- + The Banking instruction received by The Bank are unclear, defective, insufficient information;

- + The Customer's account balance or credit limit is insufficient;

- + The amount of The Customer's account is frozen or deducted in accordance with the regulations of laws;

- + The Customer does not operate in accordance with The Bank's relating professional regulations;

- + Force majeure circumstances or other problems are not caused by The Bank's fault.

- When the agreement is terminated or stopped during the validity term, The Bank will not return the relevant fees paid by The Customer;

- If The Bank's E-banking system has errors, problems or other causes those got The Customer improperly benefit, The Bank has the right to deduct such benefit from The Customer's account or

suspend E-banking service for The Customer temporarily ;

- The Bank has the right to refuse to provide E-banking services to The Customer if The Customer does not have the data submission according to the required method by this regulation;

2. Obligations

- The Bank is responsible for the legality of the related software used in E-banking;

- The Bank is responsible for promptly carrying out procedures to register E-banking services for The Customer, and providing corresponding E-banking services to The Customer according to The Customer's requests;

- The Bank is responsible for providing service guidance on E-banking to The Customer, and publishing contents such as: business introduction, inquiry – answer, transaction rules at The Bank's official website;

- The Bank may use The Customer's documents and transaction details to the extent permitted by law. The Bank is obliged to keep confidential the records and information provided by The Customer, unless other provisions provided by law;

- When The Customer registers to receive security devices and is accepted by The Bank, The Bank must promptly deliver Token Key and password to The Customer and ensure that user is frozen before delivery;

- In case The Bank's system is operating normally, The Bank is responsible for promptly handling the exact E-banking business orders received from The Customer . Services are as follows:

- + Providing The Customer with 24-hour online account inquiry service;

- + For internal VND transfer transactions within ICBC, The Bank will immediately process and credit the beneficiary's account;

- + For payment orders that the beneficiary opens another bank account in Vietnam, if that payment orders are sent before 04:00 PM on the working day, The Bank will process in the same day, if such payment orders are sent after 04:00 PM on the working day, The Bank will process at the next business day;

- + For automatic cross-border remittance instructions, The Bank will review and process on the next business day provided that the information is complete and accurate. The Customer are responsible for proactively checking the transaction status after submitting the instructions.

- The Bank reserves the right to modify or temporarily suspend services due to system upgrades or maintenance, in principle, this shall not exceed 4 times per year, with total duration of time shall not exceed 4 hours, and the Bank is obligated to notify customers of such changes or suspensions at least 5 days in advance;

- Upon receiving a feedback on E-banking service from The Customer, The Bank must promptly check and notify The Customer of the results;

Article 4 Collection and Use of Customer Information

- The Customer agrees and commits to providing the Bank with accurate, truthful, and complete information. In cases where customers refuse to provide information as requested, the Bank may consider refusing to provide services;

- The Customer consents to the Bank using, storing, and providing their information to individuals or organizations as required by law or requested by competent authorities;

- The Customer accepts and agrees that the Bank may use their information to share with third parties cooperating with the Bank for the purpose of improving service quality and customer benefits;

- The Customer agrees to comply with other rights and obligations under the Bank's General Terms and Conditions on Personal Data Protection.

Article 5 Warning of Risks

- If The Customer agrees to use E-banking service provided by The Bank, The Customer is deemed to have fully understood the risks in the transaction through the E-banking, and accept the possible losses from this system;

- The Bank makes all effective measures with the most effort to protect the safety of The Customer's documents and transactions. However, with the responsibility of The Bank to The Customer, The Customer should be specifically noted that exist risks of the E-banking service include but not limit to the following cases:

- + Storing banking information, passwords, or OTP codes on mobile devices or saving them in web browsers may create opportunities for unauthorized parties to easily access and take control of the account if the device is stolen or accessed illegally;

+ Downloading and installing applications from untrusted sources or visiting websites containing malware can cause the phone or computer to be infected with spyware, allowing attackers to monitor and steal the banking information;

+ Public Wi-Fi networks are vulnerable environments where attackers may intercept or manipulate data transmissions between users and the Bank's system. Using unsecured public Wi-Fi to access your bank account increases the risk of data compromise;

+ If the phone's operating system or the banking application is not regularly updated, the latest security patches will not be applied, making the device more vulnerable to exploitation through publicly known security vulnerabilities;

+ The Customer may unknowingly access phishing websites or messages that closely resemble the Bank's official communications (with subtly altered URLs), leading The Customer to enter personal data and inadvertently expose the account information to attackers;

+ For Corporate Customer, weak internal control policies regarding transaction approval processes or allowing unauthorized staff to perform operations may result in financial losses for which the Customer will bear full responsibility;

+ In some cases, the Bank's system may experience technical errors in transaction processing, resulting in temporary balance discrepancies or service interruptions.

- To protect The Customer's account, the Bank strongly advises The Customer to:

+ Never disclose confidential information such as usernames, account numbers, personal data, passwords, OTP codes, etc., to anyone under any circumstances;

+ Avoid clicking on unfamiliar links or downloading unofficial applications;

+ Do not conduct transactions on public/shared devices or over unsecured Wi-Fi networks;

+ Secure personal devices by installing antivirus software, enhancing device security measures such as screen/app locks, and avoiding the installation of applications from unknown sources;

+ Only install applications from official sources such as the App Store, Google Play, CH Play, or through links provided directly by the Bank;

+ Regularly monitor transaction history to detect unusual activities and immediately notify the Bank. In case of suspected fraud or signs of unauthorized account access, contact ICBC immediately for support and account suspension to prevent financial loss.

Article 6 Languages

- This General Terms and Conditions are made in Vietnamese, English and Chinese. In the event of any inconsistency, the Vietnamese version shall prevail.

ĐIỀU KHOẢN VÀ ĐIỀU KIỆN CHUNG VỀ DỊCH VỤ
NGÂN HÀNG ĐIỆN TỬ CỦA ICBC - CHI NHÁNH TP HÀ NỘI
(Bản 202505)

Điều 1 Định nghĩa

Ý nghĩa các từ ngữ được sử dụng trong Điều Khoản và Điều Kiện Chung này được giải thích như sau:

1. “Ngân Hàng điện tử” (E-banking) là dịch vụ Ngân Hàng hỗ trợ Khách Hàng tự thao tác sử dụng dịch vụ Ngân Hàng tự động thông qua mạng Internet và các thiết bị đầu cuối. E-banking của Ngân Hàng Industrial and Commercial Bank of China Limited - Chi nhánh Thành phố Hà Nội (“Ngân Hàng”) được cung cấp thông qua Internet Banking/ Mobile Banking, cho các dịch vụ quản lý tài chính như: truy vấn thông tin tài khoản, chuyển khoản, thanh toán trực tuyến và quản lý tài chính.
2. “Khách Hàng” là cá nhân, tổ chức mở tài khoản tại Ngân Hàng.
3. “Token Key” là thiết bị bảo mật tạo ra mật mã động với màn hình hiển thị và bàn phím bằng số.
4. “SMS OTP” là khi Khách Hàng thực hiện giao dịch trên Internet Banking/ Mobile Banking, hệ thống sẽ gửi tin nhắn mã khóa một lần đến số điện thoại Khách Hàng đã đăng ký.
5. “SOFT TOKEN”/ “DIGITAL TOKEN” là hình thức xác nhận được cài đặt trên ứng dụng Mobile Banking của Khách Hàng. Khi thực hiện giao dịch trên Internet Banking/ Mobile Banking, Khách Hàng nhập mã khóa SOFT TOKEN/ DIGITAL TOKEN trên ứng dụng Mobile Banking để xác nhận giao dịch.
6. “Sinh trắc học”/ “Xác thực khuôn mặt”/ “Xác thực FaceID” là biện pháp xác thực bằng dấu hiệu nhận dạng sinh trắc học của Khách Hàng khớp đúng với dữ liệu sinh trắc học được lưu trong bộ phận lưu trữ thông tin được mã hóa của thẻ căn cước công dân hoặc thẻ căn cước của hoặc dữ liệu đã được Ngân Hàng thu thập và kiểm tra.
7. “Thiết bị bảo mật” là công cụ thiết bị vật lý hoặc điện tử để xác thực Khách Hàng nhằm

đảm bảo an toàn giao dịch cho Khách Hàng.

8. “Lệnh nghiệp vụ E-banking” là các yêu cầu vắn tin tài khoản, chuyển khoản mà Khách Hàng gửi tới Ngân Hàng thông qua Internet Banking/ Mobile Banking bằng mã Khách Hàng (số thẻ) hoặc thiết bị bảo mật và mật khẩu tương ứng.

9. “Đăng ký online” là Khách Hàng tự đăng ký tài khoản Internet banking hoặc Mobile banking khi đã có tài khoản Ngân Hàng Industrial and Commercial Bank of China Limited - Chi nhánh Thành phố Hà Nội. Khách Hàng đăng ký online có thể thực hiện truy vắn tài khoản. Nếu Khách Hàng có nhu cầu thực hiện thanh toán như chuyển khoản qua Ngân Hàng điện tử có thể mở dịch vụ tại quầy Giao dịch.

Điều 2 Quyền lợi, nghĩa vụ của Khách Hàng

1. Quyền lợi

- Khách Hàng tự nguyện đăng ký sử dụng dịch vụ E-banking của Ngân Hàng, sau khi được sự đồng ý của Ngân Hàng, Khách Hàng có quyền sử dụng các dịch vụ tương ứng theo các nội dung đã đăng ký;

- Trong thời gian hiệu lực của dịch vụ, Khách Hàng có quyền thực hiện các thủ tục chấm dứt việc sử dụng dịch vụ E-banking;

- Khách Hàng được quyền lựa chọn đăng ký, thay đổi, hủy bỏ biện pháp xác thực, bao gồm nhưng không giới hạn bởi các biện pháp xác thực Token key, SMS OTP, SOFT TOKEN, DIGITAL TOKEN, Sinh trắc học và biện pháp xác thực khác do Ngân Hàng cung cấp tại từng thời kỳ;

- Khi chấm dứt hoặc ngừng sử dụng dịch vụ, Khách Hàng không cần trả lại thiết bị bảo mật. Đối với Khách Hàng đăng ký online không cần thiết bị Token Key;

- Khi xảy ra các vấn đề như sự cố mạng, sự cố viễn thông dẫn đến Khách Hàng không thể thực hiện giao dịch qua hệ thống E-banking của Ngân Hàng, Khách Hàng có thể đến Phòng Giao dịch của Ngân Hàng để thực hiện các nghiệp vụ;

- Nếu có thắc mắc, khiếu nại hoặc ý kiến về dịch vụ E-banking của Ngân Hàng, Khách Hàng có thể gọi điện thoại tới số: 18001005 (24/7), 024.62699818 / 62699830 (trong giờ làm việc) hoặc đến Phòng Giao dịch của Ngân Hàng để được tư vấn và giải đáp.

2. Nghĩa vụ

- Khách Hàng đã hiểu rõ những rủi ro có thể gặp phải trong quá trình sử dụng dịch vụ Ngân Hàng điện tử (bao gồm nhưng không giới hạn ở các rủi ro thông tin bị tiết lộ, thông tin chứng từ sai lệch, lừa đảo .v.v.), và tự nguyện chịu mọi tổn thất do những rủi ro này gây ra;

- Khách Hàng đã đọc và hiểu chính xác, đầy đủ bản Điều Khoản và Điều Kiện Chung này;

- Khách Hàng phải đảm bảo về độ an toàn và độ tin cậy của các thiết bị mà Khách Hàng sử dụng để giao dịch qua E-banking. Ngân Hàng không chịu trách nhiệm về những tổn thất kinh tế do các nguyên nhân như sự cố về thiết bị của Khách Hàng, sự cố liên lạc gây ra;

- Khi nhận thiết bị bảo mật, Khách Hàng phải xác nhận và nộp lại đơn xác nhận (đối với Khách Hàng tổ chức), thông báo cho Ngân Hàng mở khóa tài khoản Ngân Hàng điện tử;

- Khi Khách Hàng nhận thiết bị bảo mật, phải chịu trách nhiệm về mọi thao tác khi sử dụng thiết bị bảo mật, số thẻ đăng ký (ID đăng nhập) và mật khẩu liên quan. Khách Hàng Tổ Chức phải giao nhân viên chuyên trách bảo quản và sử dụng thiết bị bảo mật, thông tin đăng nhập, không được cung cấp cho người không liên quan. Đồng thời, phải căn cứ yêu cầu kiểm soát nội bộ của Khách Hàng để thiết lập hợp lý quyền hạn thao tác và hạn mức giao dịch phù hợp, nhằm đảm bảo an toàn tài khoản;

- Sau khi đã thực hiện giao dịch thành công, Khách Hàng không được sửa đổi hoặc hủy giao dịch thanh toán;

- Nếu trong thời gian còn hiệu lực mà thiết bị bảo mật bị hỏng, bị khóa, bị mất, bị lộ mật khẩu hoặc bị quên mật khẩu thì phải kịp thời làm các thủ tục đổi thiết bị bảo mật mới hoặc mở khóa, báo mất, hoặc cài đặt lại mật khẩu. Khách Hàng chịu trách nhiệm với những rủi ro có thể phát sinh trước khi thực hiện các thủ tục trên;

- Trong quá trình sử dụng dịch vụ E-banking, Khách Hàng cần chủ động, kịp thời cập nhật thông tin với Ngân Hàng khi có sự thay đổi. Khách Hàng tự chịu trách nhiệm với những rủi ro có thể phát sinh trước khi thực hiện các thủ tục thay đổi;

- Khách Hàng hiểu và đồng ý rằng Ngân Hàng có quyền thu thập thông tin sinh trắc khuôn mặt cho mục đích xác thực Khách Hàng, đăng nhập ứng dụng Mobile Banking, xác thực giao dịch và các mục đích hợp pháp khác. Khách Hàng có trách nhiệm tự bảo mật thông tin sinh trắc khuôn mặt của mình. Những tổn thất, thiệt hại phát sinh do việc Khách Hàng tự lưu trữ thông tin sinh trắc khuôn mặt sẽ do Khách Hàng tự chịu trách nhiệm;

- Khách Hàng phải đảm bảo khả năng thanh toán của tài khoản sử dụng dịch vụ E-banking và

chấp hành nghiêm chỉnh các quy định pháp luật liên quan về nghiệp vụ thanh toán. Khách Hàng là người chịu trách nhiệm cuối cùng về tính hợp pháp, hợp lệ của lệnh thanh toán, đảm bảo phù hợp với phạm vi, nội dung hoạt động theo giấy phép hoạt động (hoặc các giấy tờ tương đương khác) của Khách Hàng;

- Khi thực hiện giao dịch trên E-banking, Khách Hàng phải đảm bảo tính chân thực, sự hoàn chỉnh và chính xác của thông tin giao dịch, phải ghi rõ lý do mục đích sử dụng của khoản thanh toán đó. Khách Hàng phải chịu trách nhiệm về tính chân thực, tính hợp pháp của lý do chi trả;

- Nếu Khách Hàng phát hiện Ngân Hàng sai sót trong việc xử lý lệnh thực hiện nghiệp vụ thông qua E-banking của phải kịp thời thông báo cho Ngân Hàng;

- Khi sử dụng dịch vụ E-banking của Ngân Hàng, Khách Hàng phải chi trả các khoản phí theo biểu phí tiêu chuẩn liên quan đến dịch vụ E-banking của Ngân Hàng và đồng ý Ngân Hàng chủ động thu phí từ tài khoản của Khách Hàng;

- Khách Hàng không được lấy lý do xảy ra tranh chấp với bên thứ ba để từ chối chi trả khoản tiền phải trả cho Ngân Hàng;

- Khách Hàng không được cố ý làm tổn hại đến danh dự của Ngân Hàng hoặc tấn công hệ thống E-banking của Ngân Hàng;

- Khi Khách Hàng thực hiện giao dịch qua E-banking, nếu các chức năng dịch vụ mà Khách Hàng sử dụng liên quan đến các quy tắc hoặc quy định nghiệp vụ khác của Ngân Hàng thì Khách Hàng phải đồng thời tuân thủ các quy tắc hoặc quy định nghiệp vụ đó;

- Nếu trong thời gian dài không sử dụng E-banking, Khách Hàng cần chủ động làm thủ tục xin chấm dứt sử dụng.

Điều 3 Quyền lợi, nghĩa vụ của Ngân Hàng

1. Quyền lợi

- Ngân Hàng không chịu trách nhiệm với bất kỳ thiệt hại nào xảy ra do lỗi Khách Hàng để lộ tên truy cập, mật khẩu, thông tin, phương thức xác thực vì bất kỳ lý do gì;

- Ngân Hàng không chịu trách nhiệm nếu Khách Hàng sử dụng phần mềm, tài liệu hay tuân theo các chỉ dẫn không do Ngân Hàng cung cấp;

- Ngân Hàng có quyền lập biểu phí tiêu chuẩn dịch vụ E-banking và công bố tại trang thông tin điện tử chính thức và Phòng Giao dịch của Ngân Hàng;

- Ngân Hàng có quyền nâng cấp, cải tạo hệ thống E-banking;
- Ngân Hàng có quyền tự động thu thập thông tin thiết bị mà Khách Hàng đã tải ứng dụng để nhận dạng thiết bị nhằm phục vụ việc thẩm định, phê duyệt thiết bị đăng ký sử dụng chức năng đăng nhập và xác thực bằng sinh trắc học theo quy định của Ngân Hàng và hỗ trợ theo dõi khi cần thiết;
- Chủ động quyết định hạn mức giao dịch áp dụng với từng loại biện pháp xác thực nhằm đảm bảo an toàn, hạn chế rủi ro cho Khách Hàng cũng như tuân thủ theo các quy định pháp luật;
- Ngân Hàng được miễn trừ mọi trách nhiệm phát sinh từ việc thiết bị của Khách Hàng đăng ký/lưu trữ sinh trắc học của người khác;
- Ngân Hàng có quyền đơn phương chấm dứt cung cấp dịch vụ Ngân Hàng điện tử cho Khách Hàng trong những trường hợp sau đây: (i) Khách Hàng không tuân thủ các quy định liên quan của pháp luật và của Ngân Hàng ; (ii) Thực hiện theo yêu cầu của cơ quan chức năng; (iii) Khách Hàng có hành động xấu, làm tổn hại đến danh tiếng của Ngân Hàng; (iv) Ngân Hàng phát hiện có rủi ro giả mạo, lừa đảo; (v) Khách Hàng không thanh toán các chi phí đúng thời hạn; (vi) Khách Hàng có tài khoản không sử dụng trong thời gian dài theo quy định tại “Điều khoản và điều kiện chung về sử dụng tài khoản” hiện hành của Ngân Hàng; (vii) Một năm kể từ thời điểm Khách Hàng đăng ký dịch vụ Ngân Hàng điện tử nhưng chưa hoàn tất thủ tục nhận thiết bị bảo mật;
- Ngân Hàng căn cứ vào thời gian và thông tin thao tác trên Ebanking của Khách Hàng làm căn cứ xử lý nghiệp vụ;
- Nếu xảy ra một trong các tình huống dưới đây dẫn đến Ngân Hàng không thể thực hiện được chính xác lệnh nghiệp vụ E-banking mà Khách Hàng đề nghị thì Ngân Hàng không phải chịu bất kỳ trách nhiệm nào:
 - + Lệnh nghiệp vụ mà Ngân Hàng nhận được không rõ ràng, bị lỗi, thông tin không hoàn chỉnh;
 - + Số dư tài khoản hoặc mức tín dụng của Khách Hàng không đủ;
 - + Số tiền trong tài khoản của Khách Hàng bị phong tỏa hoặc bị khấu trừ theo quy định của pháp luật;
 - + Khách Hàng không thao tác đúng theo các quy định về nghiệp vụ liên quan của Ngân Hàng;
 - + Xảy ra các tình huống bất khả kháng hoặc các vấn đề khác không phải do lỗi của Ngân Hàng.

- Khi thỏa thuận chấm dứt hoặc ngừng trong thời gian còn hiệu lực thì Ngân Hàng không trả lại các chi phí liên quan mà Khách Hàng đã nộp;

- Nếu do hệ thống E-banking của Ngân Hàng bị lỗi, gặp sự cố hoặc các nguyên nhân khác làm cho Khách Hàng được lợi không chính đáng, Ngân Hàng có quyền khấu trừ các khoản thu lợi không chính đáng từ tài khoản của Khách Hàng hoặc tạm ngừng dịch vụ E-banking của Khách Hàng;

- Ngân Hàng có quyền từ chối cung cấp dịch vụ Ngân Hàng điện tử cho Khách Hàng nếu Khách Hàng không truyền dữ liệu theo phương thức yêu cầu trong quy định này.

2. Nghĩa vụ

- Ngân Hàng chịu trách nhiệm về tính hợp pháp của các phần mềm liên quan sử dụng trong E-banking;

- Ngân Hàng chịu trách nhiệm kịp thời thụ lý đăng ký dịch vụ E-banking cho Khách Hàng, và cung cấp dịch vụ E-banking tương ứng theo nhu cầu của Khách Hàng;

- Ngân Hàng chịu trách nhiệm cung cấp tư vấn dịch vụ về E-banking cho Khách Hàng, và công bố các nội dung như: giới thiệu nghiệp vụ, hỏi đáp, các quy tắc giao dịch tại cổng thông tin điện tử chính thức của Ngân Hàng;

- Ngân Hàng được sử dụng tài liệu và chi tiết giao dịch của Khách Hàng trong phạm vi cho phép của pháp luật. Ngân Hàng có nghĩa vụ giữ bí mật các tài liệu hồ sơ và thông tin mà Khách Hàng cung cấp, trừ trường hợp có quy định khác của pháp luật;

- Khi Khách Hàng đăng ký nhận thiết bị bảo mật và được Ngân Hàng chấp nhận, Ngân Hàng phải kịp thời giao thiết bị bảo mật cho Khách Hàng;

- Trong trường hợp hệ thống của Ngân Hàng đang vận hành bình thường, Ngân Hàng chịu trách nhiệm kịp thời xử lý chuẩn xác lệnh nghiệp vụ E-banking mà Khách Hàng gửi. Dịch vụ được cung cấp như sau:

+ Cung cấp cho Khách Hàng dịch vụ vắn tin tài khoản 24/24 giờ;

+ Đối với lệnh thanh toán Việt Nam đồng trong hệ thống, Ngân Hàng sẽ lập tức xử lý và ghi có vào tài khoản của người thụ hưởng;

+ Đối với những lệnh thanh toán mà người thụ hưởng mở tài khoản tại Ngân Hàng khác tại Việt Nam, đồng thời thông qua hệ thống chuyển khoản liên Ngân Hàng, nếu gửi trước 16:00 trong ngày làm việc, Ngân Hàng sẽ xử lý ngay trong ngày, nếu gửi sau 16:00 trong ngày làm việc, Ngân

Hàng sẽ xử lý vào ngày làm việc tiếp theo;

+ Đối với những lệnh thanh toán nước ngoài tự động sẽ được kiểm duyệt và xử lý vào ngày làm việc tiếp theo nếu thông tin đầy đủ và chính xác. Khách Hàng cần chủ động kiểm tra trạng thái giao dịch sau khi hoàn tất gửi lệnh.

- Ngân Hàng có quyền thay đổi, tạm ngừng cung cấp dịch vụ do hệ thống nâng cấp, sửa chữa. Tuy nhiên về nguyên tắc, số lần thay đổi, tạm ngừng thực tế không vượt quá 04 lần/năm, với tổng thời gian không vượt quá 04 giờ, và Ngân Hàng có trách nhiệm thông báo cho Khách Hàng về việc thay đổi, tạm ngừng trước 05 ngày;

- Khi nhận được phản ánh về dịch vụ E-banking từ Khách Hàng, Ngân Hàng phải kịp thời tiến hành kiểm tra và thông báo cho Khách Hàng biết kết quả kiểm tra.

Điều 4 Thu thập và sử dụng thông tin của Khách Hàng

- Khách Hàng đồng ý và cam kết cung cấp cho Ngân Hàng các thông tin chính xác, trung thực, đầy đủ. Trường hợp Khách Hàng từ chối cung cấp thông tin theo yêu cầu, Ngân Hàng có thể xem xét việc từ chối cung cấp dịch vụ;

- Khách Hàng đồng ý để Ngân Hàng sử dụng, lưu trữ, cung cấp thông tin Khách Hàng cho những cá nhân/ tổ chức theo quy định của pháp luật hoặc theo yêu cầu của cơ quan có thẩm quyền;

- Khách Hàng chấp nhận, đồng ý và cho phép Ngân Hàng sử dụng thông tin Khách Hàng để chia sẻ cho bên thứ ba có hợp tác với Ngân Hàng nhằm nâng cao chất lượng phục vụ và lợi ích của Khách Hàng;

- Khách Hàng đồng ý thực hiện các quyền và nghĩa vụ khác theo các Quy định chung về Bảo vệ dữ liệu cá nhân do Ngân Hàng quy định.

Điều 5 Cảnh báo về rủi ro

- Nếu Khách Hàng đồng ý đề nghị sử dụng dịch vụ E-banking do Ngân Hàng cung cấp, Khách Hàng được coi là đã hoàn toàn hiểu về các rủi ro trong giao dịch thông qua Ngân Hàng điện tử, và chấp nhận những thiệt hại có khả năng xảy ra từ hệ thống này;

- Ngân Hàng sử dụng tối đa mọi biện pháp hữu hiệu để bảo vệ sự an toàn cho tài liệu chứng từ và hoạt động giao dịch của Khách Hàng. Mặc dù vậy, với trách nhiệm đối với Khách Hàng, Ngân

Hàng đặc biệt lưu ý với Khách Hàng rằng, những rủi ro tồn tại trong dịch vụ Ngân Hàng điện tử bao gồm nhưng không giới hạn các trường hợp dưới đây:

- + Việc lưu thông tin tài khoản Ngân Hàng, mật khẩu, mã OTP trên điện thoại hoặc ghi chú trong trình duyệt web có thể tạo cơ hội cho kẻ gian dễ dàng chiếm đoạt tài khoản khi thiết bị bị đánh cắp hoặc truy cập trái phép;

- + Việc tải và cài đặt ứng dụng từ các nguồn không đáng tin cậy hoặc truy cập vào các trang web chứa mã độc có thể khiến điện thoại/máy tính bị nhiễm phần mềm gián điệp, từ đó kẻ gian sẽ theo dõi và đánh cắp thông tin tài khoản Ngân Hàng;

- + Wi-Fi công cộng là môi trường dễ bị tấn công, kẻ gian có thể theo dõi, can thiệp vào dữ liệu truyền tải giữa người dùng và hệ thống Ngân Hàng nếu người dùng sử dụng Wi-Fi công cộng thiếu độ tin cậy để truy cập vào tài khoản Ngân Hàng;

- + Khi hệ điều hành điện thoại hoặc ứng dụng Ngân Hàng không được cập nhật thường xuyên, các bản vá bảo mật mới sẽ không được áp dụng, khiến thiết bị dễ bị khai thác các lỗ hổng bảo mật đã được công bố công khai;

- + Khách Hàng có thể vô tình truy cập vào các trang web giả mạo hoặc tin nhắn lừa đảo có nội dung gần giống với Ngân Hàng thật (địa chỉ URL có ký tự thay đổi tinh vi), từ đó nhập thông tin cá nhân và bị kẻ gian chiếm đoạt thông tin tài khoản;

- + Đối với Khách Hàng là tổ chức, quy định quản lý nội bộ thiếu chặt chẽ đối với quy trình thẩm duyệt nghiệp vụ và các lệnh nghiệp vụ do nhân viên không có thẩm quyền của Khách Hàng thao tác có thể dẫn đến những tổn thất tài chính mà Khách Hàng sẽ phải tự chịu trách nhiệm.

- + Trong một số trường hợp hệ thống Ngân Hàng có thể gặp lỗi xử lý giao dịch, gây sai lệch số dư tạm thời hoặc gián đoạn dịch vụ.

- Để bảo vệ an toàn tài khoản, Ngân Hàng khuyến cáo Khách Hàng:

- + Không cung cấp thông tin bảo mật như tên truy cập, số tài khoản, thông tin cá nhân, mật khẩu, mã OTP, vv cho bất kỳ ai dưới bất kỳ hình thức nào;

- + Không truy cập vào các đường dẫn lạ hoặc tải các ứng dụng không chính thống;

- + Không thực hiện giao dịch trên thiết bị công cộng hoặc khi đang dùng Wi-Fi không bảo mật;
- + Bảo mật thiết bị cá nhân: Cài đặt phần mềm diệt virus, nâng cấp các biện pháp bảo mật thiết bị như khóa màn hình và khóa ứng dụng, không cài ứng dụng không rõ nguồn gốc;
- + Chỉ cài đặt ứng dụng từ các nguồn chính thống như App Store, Google Play, CH Play hoặc đường dẫn do Ngân Hàng cung cấp;
- + Kiểm tra thông tin giao dịch thường xuyên nhằm phát hiện bất thường và thông báo ngay cho Ngân Hàng. Khi nghi ngờ bị lừa đảo hoặc có dấu hiệu xâm nhập tài khoản hãy lập tức liên hệ ICBC để được hỗ trợ và phong tỏa tài khoản kịp thời để ngăn chặn các tổn thất về tài sản.

Điều 5 Ngôn ngữ

Bản Điều khoản và Điều kiện Chung này được lập bằng ngôn ngữ tiếng Việt, tiếng Anh và tiếng Trung. Trong trường hợp có bất kỳ sự không thống nhất giữa các ngôn ngữ, bản tiếng Việt sẽ được ưu tiên áp dụng.