GUIDELINES FOR SAFE ONLINE BANKING AND CARD TRANSACTIONS

In order to ensure information security, protect the rights and interests of customers when using the Online Banking and Card services of Indovina Bank Limited (IVB), please carefully read and comply with the following instructions:

I. GUIDELINES FOR SAFE TRANSACTIONS ON ONLINE BANKING CHANNEL

1. Principles of information security:

CUSTOMERS SHOULD NOT:

- Open an account and register Online banking services for others to use
- Write down your username and password on paper or save it automatically on a web browser or save it in any unsafe form to prevent information from being exposed.
- Provide Online Banking information (username/ password/ OTP password/ OTP code, Soft Token, PIN, etc.) to anyone in any form (phone, email, social network, application, link, word), ect.
- Log in/ declare personal information/ enter OTP on strange links/ websites of unknown origin, especially:
  - The links attached in the emails are suspected to be fake, SMS, social networking applications.
  - Incoming phone calls ask you to follow instructions to access unfamiliar websites or install applications from unknown sources.

  IVB never actively asks you to provide their usernames and passwords to access Online Banking services via phone, email or any other form. Any request for service security information is fake.
- Installing strange software, uncopyrighted software, software of unknown origin;
- Use mobile devices that have been broken to download and use the Online Banking application software, OTP generation software.
- Leave or allow others to use computers, mobile devices, and authentication devices until successfully logged out of the service.
- Use public computers to access and perform transactions; use public Wifi networks when using Online Banking services.
- Transfer money, top up to the designated phone number to carry out the procedures for receiving rewards. IVB never asks you to transfer money, top up phone numbers to receive any IVB promotions.
- Follow the instructions of the messages requesting money transfer to serve the investigation (drug smuggling, money laundering, etc.) to prove innocence or transfer money to prove the loan, support SIM upgrade, support biometric installation, etc. because these are scam calls.

CUSTOMERS SHOULD:

About setting up passwords and PINs:

- Set up a strong password**:** At least 08 characters long, a combination of uppercase letters, lowercase letters, numbers and special characters.
- Service access passwords: not shared/t he same as passwords used by other services: computer passwords, facebook, email, zalo, viber, etc.
- Do not use access passwords that are easy for others to guess such as: personal information such as date of birth, phone number, citizen ID, license plate, identity card, personal name, name of relatives such as spouse/ child, simple continuous number sequence such as 123456, etc.
- Set up and use a secure PIN (Personal Identification Number): When setting up an PIN code or Soft OTP, don't use consecutive sequences of numbers, repeating numbers, or easy-to-guess personal information.

About password and PIN security:

- Change your password to access Online Banking services for the first time within 24 hours from the date of receipt and change your password regularly (at least every 06 months).
- Change immediately after discovering that you have just clicked on links that are suspected to be fake or accidentally reply to information to strangers calling or when exposed, suspected to be exposed to ensure the safety of your account.
- Never share your PIN with anyone in any way.

2. Principles of safe use of services:

- Only download and log in to IVB Mobile Banking application, IVB Biz+ which has been confirmed on the App Store or Google Play and the official Internet Banking address on the website: www.indovinabank.com.vn.

IVB Indovina Bank logo on App store IVB

Indovina Bank logo on Google Play

- Only sign in through trusted devices. Using computers/ mobile devices with full installation of security vulnerability patches of the operating system and IVB Mobile Banking and IVB Biz+ application software; review and regularly update antivirus software and firewalls.

Regularly delete your web browser's history, cache, cache, and files generated by websites you visit (cookies) of your web browser.

- To use the Online Banking service, please visit IVB's official website at the www.indovinabank.com.vn and select "Log in to Internet Banking" or download the IVB Mobile Banking/ IVB Biz+ application on App Store or Google Play.
- When receiving an OTP message from IVB, it is necessary to carefully check the content of the message, including: transaction type, transaction amount, transaction channel. If the content of the message does not match the transaction being made, you absolutely do not enter this OTP code into any device or disclose it to anyone.
- When the system is processing a transaction, do not exit the trading screen and wait for the result notification from the system before executing other trades.
- Always remember to Log out of your device after each access to Online Banking services.
- It is recommended to register to use banking services via IVB SMS Banking and turn on the notification popup on mobile devices to receive notifications of balance fluctuations to help you immediately know the transactions on the account, limiting risks and losses to the lowest level.
- In case of not making a transaction but still receiving a notification from IVB about: OTP code; abnormal balance changes; activate the app on another device; E-wallet linking, etc. You immediately notify IVB and do not provide the above information to anyone and in any form.

II. GUIDELINES FOR SAFE TRANSACTIONS WITH IVB CARD

1. General principles:

When receiving the card, customers need to do:

- Check that the name on the card is the same as the name you have registered.
- Immediately change your PIN for debit cards (ATMs) provided by the bank at ATMs.
- Do not set passwords related to personal information such as: Date of birth, phone number, license plate, citizen ID, etc.
- Do not write passwords on the card or near the place where the card is stored to avoid information disclosure and being taken advantage of.

Always keep your card and PIN, card confirmation number confidential in all cases:

- Do not give your card to any person other than the bank's staff or the merchant's cashiers appointed to work with you.
- Do not disclose the information printed on the front and back of the card as well as the PIN number and confirmation number to anyone. You are the only one who knows that information.
- Do not disclose transaction information to anyone.

When making a transaction using PIN, customers should note:

- Make sure no one sees the PIN when making a transaction (by covering the keyboard);
- It is recommended to change the PIN number frequently.

- If the PIN is entered incorrectly 03 times in a row, the card will be locked on the transaction day to ensure absolute safety for you.

Register and use IVB's Online Banking services (IVB Mobile Banking, IVB Biz+, SMS Banking...) to ensure:

- Be notified of fluctuations related to your personal account or card limit as soon as a card transaction is made.
- Actively lock/ unlock the internet spending feature for international credit cards/ international debit cards/ domestic debit cards to control online payment transactions.

2. Principles of card preservation:

- Do not bend the card, fold the card.
- Do not leave the card near electronic devices that can broadcast, strong magnetism can damage the data on the card.
- Keeping the card carefully and checking regularly helps you detect when the card is lost early.

3. Principles when transacting at ATMs:

- Carefully observe ATMs before making transactions, especially at the following locations: card reader slots, keyboards, cameras. If you notice that the ATM has strange devices or any abnormal signs, you should stop the transaction and immediately notify the following:
  - At IVB's ATMs: Contact the hotline 1900 588 879 immediately.
  - At ATMs of other banks: Immediately contact the hotline number posted on that ATM.

  At the same time, you should go to the nearest IVB branch/ transaction office to change the card to prevent the risk of information leakage.
- It is recommended to cover the keyboard with your hand when entering the PIN password.
- You use the card according to the instructions at the ATM, the ATM will release the money first and give the card later, you should wait for the machine to dispense the money, do not leave immediately to avoid the case that the ATM is slow to release money and others can take this money.

4. Principles when paying by card at Merchants:

- Pay attention to check the information on the card payment invoice, make sure the information is accurate and complete. Only sign for payment when agreeing on all the information on the invoice.
- Ensure that all card transactions at merchants must be conducted in front of you.
- Guaranteed to receive the card back after completing the transaction at merchants.
- Retain the card payment invoices and relevant documents to serve the future tracing of complaints (if any).

5. Principles when transacting cards for payment on the Internet:

- Only use card information to make payments at websites certified by Visa/Master (write "Verified by Visa/Master") and have additional OTP password authentication of 3D Secure service, do not use public computers when making online payment transactions.
- Read the unit's policies carefully before agreeing to payment.
- Always remember to Log out of the website after the end of the transaction.

- After completing the online payment transaction, actively lock the Internet spending feature of the card by using the online card unlocking service via IVB Ebanking/ IVB Mobile Banking/ IVB Biz+ or call 1900 588 879 for support.

III. WARNING OF ONLINE AND CARD FRAUD

In order for you to actively prevent risks and minimize losses, IVB lists here some common tricks that criminals often use today:

- Impersonating competent agencies (police, courts, tax authorities, etc.) to send fake links/ websites to fake public services for you to install fake applications (VNeID application, application of the General Department of Taxation, etc.), thereby hijacking control of devices, secretly stealing banking service security information and transferring money in your accounts.
- Impersonating competent agencies (courts, police, etc.) to threaten you involved in illegal acts (causing traffic accidents, related to money laundering lines, smuggling, debts for international telecommunications charges, etc.) and asking you to follow instructions (opening new accounts, providing information, installing applications, transferring money to the designated account, etc.).
- Forging the bank's website/application software/ fanpage/ SMS and sending fake links for you to enter information. Or pretending to be a bank employee to contact you to ask for support (support for faulty money transfer transactions, support for tracing, etc.) and then ask you to provide confidential information to commit the act of appropriating assets.
- Impersonating businesses, organizations notifying customers of winning promotional prizes, receiving promotional codes... and ask you to provide confidential information for banking services or transfers.
- Stealing access information on social networking platforms (Facebook, Zalo, etc.) of your friends and relatives, thereby contacting you to request money transfers for support and loans.
- **Skimming:** is a method of stealing card account information when transacting at ATMs. The criminals use very sophisticated electronic devices to steal information in ATM cards and record customers' PINs, so that they can make fake cards and withdraw customers' money from ATMs.
- **Phishing:** used as a fake website name to trick customers into logging in to take advantage of and infringe on customers' finances and information.
- **Hacking:** illegal access to customers' computers, stealing personal information, access information for illegal use
- **Deepfake/ AI phishing:** This is an extremely dangerous and explosive form. The criminals copy voice cloning or deepfake videos) of relatives, friends or partners to make video calls to borrow money, request urgent transfers, etc.

IV. SECURITY SOLUTIONS AT IVB

- To ensure safety when performing Online Banking transactions, in addition to the password when logging in, you need additional authentication such as: OTP via SMS, Soft OTP and/ or digital signature. This mechanism ensures that even if the password is exposed, the transaction cannot be carried out without a second authentication step - helping to protect your account comprehensively.
- Biometric authentication: compare facial biometric data to ensure that yourself when making online money transfer transactions over VND ten million in accordance with the regulations of the State Bank.
- Automatic account locking mechanism: After 05 unsuccessful login attempts, IVB will temporarily lock your account. To reactivate the account, you need to contact the nearest IVB Branch/ Transaction Office for instructions.
- 3D Secure solution: Provides an additional layer of cryptographic protection that you must perform to be approved when transacting on the Internet. 3D Secure solution is applicable when you make transactions on Visa/ Master's authenticated websites
- From March 1st, 2026, according to Circular 77/2025/TT-NHNN, the Mobile Banking application will automatically stop working if it detects that the mobile device is insecure, has been rooted/jailbroken, or has malware installed. This measure aims to enhance security and protect your assets from high-tech crime.
- Other solutions are implemented synchronously in the stages of service design and operation based on modern and advanced technology platforms and risk warning modes that meet international practices.

V. CONTACT IVB

Please contact IVB in the following cases:

- When encountering any errors and problems during the use of the service;
- If the phone is lost or there is any change in the phone number registered to be used associated with the service;
- When there is any change in citizen ID, email address, telephone number, residential address, address to receive card statements, signature;
- When the card is stolen, misplaced, or detected card transactions not made by the you;
- When suspecting that the email address or phone number being used is being used for illegal services;
- Accidentally clicking on suspected links or answering information over the phone with suspected impersonators;
- When there are any concerns, questions or concerns about the service and how to use IVB's card and Online Banking services;
- Actively lock the service and change the password of the service on Internet Banking or IVB Mobile Banking, IVB Biz+;
- Loss or damage to the device to generate OTP codes/ receive SMS OTP;

- Detecting fraud or suspected fraud (For example: Receiving impersonation calls requesting money transfers for investigation, installing fake biometric applications, paying for SIM upgrades, etc.);
- Being attacked by hackers or suspected of being attacked by hackers (For example: Suddenly receiving an OTP code, another device activation notification, e-wallet linking notification, or balance fluctuation even though not making a transaction, etc.).

Contact information:

- If you detect any suspicious signs of fraud or scams, please contact IVB immediately via the following channels for prompt assistance:
  - Hotline: **1900 588 879**
  - Email: **support@indovinabank.com.vn**
  - Or **IVB transaction offices** nationwide
- In any case, the only phone number of IVB Customer Service Center 24/7 to call your phone is 1900 588 879

We sincerely thank you for always trusting and using IVB's services!