

“APPROVED”
Deputy Chairman
of the Management Board of
JSC “InFinBANK”
Karimov R.A.

«_____» _____ 2025 year

Rules of JSC “InFinBank” on the use of Card Token

These Rules of JSC “InFinBank” on the use of the Card Token (hereinafter referred to as the Rules) are a public offer addressed to JSC “InFinBank”, address: Republic of Uzbekistan, 100029, Tashkent city, T. Shevchenko street, 1 (hereinafter referred to as the Bank), to an indefinite number of persons and become binding for the Client upon joining them in the manner set forth below.

Terms and definitions

NFC (Near Field Communication)	short-range (up to 10 cm) wireless high-frequency communication technology enabling contactless data exchange between devices located at short distances: for example, between a reader terminal and a cell phone, provided by the Bank in accordance with the procedure and under the terms and conditions stipulated by these Rules.
Card	JSC “InFinBank” bank card, physical or virtual, belonging to VISA, Mastercard and UnionPay payment systems, issued in national or foreign currencies.
Holder	the person in whose name the Card was issued.
Mobile device	an electronic device (tablet, smartphone, cell phone, smart watch, etc.) in the Customer's personal use that has a connection to mobile (mobile radio-telephone) communication and/or information and telecommunication network “Internet” (hereinafter referred to as the Internet).
Mobile payment service (Pay services)	service allowing to use the Mobile device of the Cardholder to conduct transactions using the Token.
Contactless payment	a method of making a payment using a Card Token by bringing or touching an NFC-enabled Mobile Device close to a reader without physical contact with the device.
Token	a unique digital identifier replacing information about the Card and its details. The Token is bound to the specific device of the Cardholder through which Tokenization was performed.
Tokenization	the process by which a Token is created.
Agreement	previously concluded between the Bank and the Customer, by signing or accepting the Bank's offer, the Bank Card Issuance and Maintenance Agreement.
Card details	Card number, Card expiration date, name and surname of the Holder (if any), Card authentication code PPC2/CVC2/CVV2.

Card Token Usage Rules

1. Tokenization of the card is possible if the following conditions are met and the requirements below are fulfilled:
 - availability of NFC function in the Mobile Device;

- only for valid (active, unblocked) payment cards issued by the Bank in the Customer's name;
 - availability of the Payment mobile service on the Mobile device;
 - is carried out by the Cardholder independently;
 - does not entail changes in the terms of use and service of the Card.
2. The Card Token is created by performing a number of actions provided by the procedures of the respective Payment Mobile Service.
 3. For one Card, it is possible to create several Tokens used in different Mobile Devices at the same time. A Token generated on one Mobile Device cannot be used on another device.
 4. the Token can be used to conduct transactions at service points equipped with terminals with the function of contactless payments, as well as in the Internet. At these service points the Cardholder should select the Token of the corresponding payment Card in the Payment Mobile Service and bring the device to the terminal (transactions will be carried out by the contactless payment principle using the payment Card). Carrying out transactions in the Internet using the Token is possible if the service point accepts payment using the Token, in this case manual entry of payment card details is not required.
 5. Transactions using the Token shall be equal to transactions using the Payment Card or its details.
 6. All conditions and requirements of the Agreement shall apply to the transactions performed using the Token.
 7. The security of using the Token is ensured by the Cardholder himself/herself. The Cardholder is recommended to:
 - not to tokenize payment cards on Mobile devices owned by third parties;
 - not to pass the Mobile Device for use by third parties;
 - delete the Token from the Mobile Device if its use is terminated;
 - in case of loss or theft of the Mobile device, as well as in case of unauthorized access to it or Token, immediately notify the Bank about the need to block the Token and/or payment card by applying to the Bank's branches or calling the Bank's Contact Center (the Bank's details are available at www.infinbank.com).
 8. Blocking of the Token or its removal from the Payment Mobile Services will be carried out by the Cardholder independently. Blocking of the Token is not the basis for blocking of the Card, to which the Token is formed.
 9. Blocking of the Card is the basis for blocking of the Token and the Token is canceled.
 10. The Bank may refuse to tokenize the Card if there are reasons to believe that the use of the Token may entail violation of the legislation, requirements of international payment systems, or a threat to information security.
 11. For information security purposes, the Bank shall be entitled to keep records (logging) of all actions related to creation, use, deletion and blocking of the Token, including recording of IP addresses, devices, time of transactions and services used.
 12. The Cardholder is fully responsible for all transactions made with the use of the Token, until the blocking of the Token and/or payment Card takes effect. In case of transferring the Mobile Device to third parties, the Holder is fully responsible for all transactions made with the use of the Token, regardless of the fact of granting consent. The Bank is not obliged to verify the authorization of the person using the Token and considers all transactions confirmed from the Mobile Device as valid.

13. The Cardholder is fully responsible for all transactions made using the Token until the Bank receives proper notification of the Token compromise, loss/theft of the Mobile Device or unauthorized access to it. In case of delayed notification, the Bank shall not be liable for any losses incurred as a result of unauthorized use of the Token.
14. The Bank shall not be liable for the inability to use the Token for reasons related to the actions/inaction of third parties (owners of mobile OS platforms, telecom operators, etc.) or due to technical failures, hacker attacks or force majeure.
15. The Bank shall not be liable for losses of the Cardholder arising as a result of:
 - transferring the Mobile Device to third parties;
 - use of compromised or outdated software;
 - violation of the terms of these Rules by the Cardholder;
 - failures in operation of operating systems, data transmission networks, program components of Payment mobile services. These losses shall not be reimbursed by the Bank.
16. Bank reserves the right:
 - at any time request confirmation of the Holder's identity and/or additional authentication (including biometric, code, multi-factor), in order to increase the level of security before tokenization and/or use of the Token;
 - at its discretion, limit the list of transactions available when using the Token, including but not limited to: cash withdrawals, transfers, international payments and/or high-risk transactions;
 - suspend or terminate the use of the Token in respect of an individual Cardholder at the request of state authorities, law enforcement and regulatory bodies or international payment systems;
 - suspend the use of the Token in case of exceeding the allowed limits on the Card, detection of attempts to bypass tariffs or in case of arrears on the bank product associated with the Card;
 - terminate, block or suspend all or some of the Tokens at any time in its sole discretion without cause and without prior notice to the Holder;
 - unilaterally amend or supplement these Regulations with placement of the updated version on the Bank's website: www.infinbank.com.
17. Notification of the Cardholder about the cancellation or suspension of the Token may be carried out at the discretion of the Bank through available communication channels, but is not its obligation.
18. Upon receipt of an application from the Cardholder about an unauthorized transaction using the Token, the Bank shall be entitled to initiate an internal investigation. The term of consideration of the application is up to 30 calendar days. Until the end of the review, the transactions are considered valid.
19. The Cardholder agrees that the Bank is not responsible for the functioning of the Payment Mobile Service and impossibility to conduct transactions using the Token.
20. The use of the Token outside the Republic of Uzbekistan is carried out by the Cardholder at his/her own risk. The Bank does not guarantee the operability of the Payment Mobile Service and compatibility with the infrastructure of foreign merchants or telecommunication operators.
21. In case of deleting the Mobile Payment Service, resetting the Mobile Device or selling/giving it to a third party, the Cardholder is obliged to delete all Tokens associated with the device in advance. In case of breach of this obligation, all related risks shall be borne by the Cardholder.

22. When tokenizing and using the Token, the Cardholder's personal data may be processed, including information about transactions, device model and serial number, geolocation and biometric data (if biometric authentication is used). The Cardholder gives his/her consent to such processing for the purposes of fulfillment of the Agreement, security enhancement and fraud prevention.
23. Refund of funds on disputable operations, made with the use of Token, is carried out in the order, provided by the card service agreement and the current legislation. Availability of the Token does not expand the rights of the Cardholder to refund.
24. The Bank may cancel the Token in case of:
 - termination of the card,
 - suspicion of fraud,
 - court injunction,
 - violation of these Rules,
 - request of state authorities.
25. In case of termination of the Bank Card Service Agreement, all previously created Tokens will be canceled. The use of Tokens after the date of termination is considered unauthorized and may result in blocking of the device and/or application to law enforcement authorities.
26. The Cardholder's actions on Tokenization of the Card means familiarization and agreement with these Rules.
27. The updated edition of the Rules is considered to be brought to the attention of the Cardholder from the moment of placement on the official website of the Bank and comes into force from the moment specified in it. Continued use of the Token after the changes come into force is considered the Holder's consent to such changes.
28. Each creation of a new Token means the Cardholder's consent to the current version of these Rules posted on the Bank's official website.

AGREED:

Murodov H.G.

full name

sign

Bagdasarov B.G.

full name

sign

Elie A.N.

full name

sign

PREPARED:

**Acting Director of Retail Business
Department**

title

Davronov B.A.

Full name

sign

REVIEWED:

Gimadieva E.Yu.

full name

sign