"Approved" by the Board of Directors of "Dos-Credobank" OJSC Minutes No. 10(9) dated 28.02.2025

REGULATION ON ELECTRONIC DOCUMENT MANAGEMENT AND THE USE OF ELECTRONIC DIGITAL SIGNATURE IN DOS-CREDOBANK OJSC

I. GENERAL PROVISIONS

1. This Regulation “On electronic document management and the use of electronic digital signatures in Dos-Credobank OJSC” (hereinafter referred to as the Regulation) regulates the procedure for organizing, maintaining and monitoring electronic document management and the use of electronic digital signatures in Dos-Credobank OJSC (hereinafter referred to as the Bank).
2. Electronic documents signed with an electronic digital signature (simple or qualified electronic signature) have legal force equivalent to paper documents in accordance with the legislation of the Kyrgyz Republic.
3. The Regulation is aimed at ensuring the security, efficiency, and transparency of electronic document management processes within the Bank, as well as in interactions with clients, authorized government agencies of the Kyrgyz Republic, and the Bank's partners/counterparties.
4. Electronic document management may be used in any of the Bank's activities, including, but not limited to: interaction with government agencies, the National Bank of the Kyrgyz Republic, the Bank's partners and counterparties, and clients (including in documents/information that were transferred by clients to the Bank or created by the Bank, or otherwise arose in connection with the Bank's relationship with clients, including their pre-contractual relations, in the course of banking activities).
5. The following terms and definitions are used within the framework of this Regulation:
   - **Electronic document management** is the process of creating, signing, transmitting, storing and processing electronic documents.
   - **An electronic document** is documented information presented in electronic form, that is, in a form suitable for human perception, using electronic computers.
   - **An electronic digital signature** is information in electronic form that is attached to and/or logically linked to other information in electronic form and that is used to identify the person on whose behalf the information is signed.
   - **Electronic document management system (Electronic document management system)** is a software and hardware complex used by the Bank to manage electronic documents.

II. BASIC PRINCIPLES OF ELECTRONIC DOCUMENT MANAGEMENT AND APPLICATION OF ELECTRONIC DIGITAL SIGNATURE

6. To successfully implement electronic document management and electronic digital signatures, which are important tools in the Bank's digital transformation and ensure the efficiency, security, and legal validity of documents, the following principles must be observed:

6.1. *Principles of electronic document management:*

6.1.1. Legality and compliance with regulatory requirements of the legislation of the Kyrgyz Republic.
   - Electronic documents must be created, transferred, stored and destroyed in accordance with the legislation of the Kyrgyz Republic.
   - The technologies used for electronic document management must comply with the

requirements of security, confidentiality and relevance standards.

6.1.2. Legal significance and reliability.

- Electronic documents must contain all required details confirming their authenticity.
- The use of an electronic digital signature on electronic documents ensures their immutability and the authorship of the owner. Electronic digital signature.

6.1.3. Security and data protection.

- Electronic documents must be protected from unauthorized access, modification and destruction.
- When creating and using electronic documents, it is recommended to use certified information security and encryption tools.

6.1.4. Efficiency and efficiency.

- Automated document flow reduces document approval times and increases employee productivity and efficiency.
- Duplication of information and manual document processing are eliminated, which reduces the risk of errors.

6.1.5. Transparency and control.

- All transactions with electronic documents are recorded in Electronic Document Management systems, ensuring their safety and control.
- Access control mechanisms and user rights delimitation are being implemented.

6.1.6. Long-term storage and archiving.

- Electronic documents must be stored in accordance with the established storage periods in accordance with the requirements of the legislation of the Kyrgyz Republic1.
- Archives are protected from loss, damage and unauthorized modification.

6.2. *Principles of using electronic digital signature:*

6.2.1. Reliability and uniqueness.

[1] *" List of the main documents generated in the activities of commercial banks and financial credit organizations licensed by the National Bank of the Kyrgyz Republic, indicating storage periods" No. 22/9 dated August 27, 2004*

- The right of participants in electronic interaction to use, at their own discretion, any type of electronic signature, if the requirement to use a specific type of electronic signature in accordance with the purposes of its use is not provided for by legislative acts, regulatory legal acts of the Kyrgyz Republic (in cases where legislative acts provide for such a possibility) or an agreement of the participants in electronic interaction;

- The possibility for participants in electronic interaction to use, at their discretion, any technology and (or) technical means that allow them to comply with the requirements of the Law of the Kyrgyz Republic "On Electronic Signatures" in relation to the use of specific types of electronic signatures;
- An electronic digital signature must guarantee the authenticity of the signatory and the integrity of the document;
- Electronic digital signature keys are stored in secure environments and are not transferred to third parties;
- It is inadmissible to recognize an electronic signature and (or) an electronic document signed with it as having no legal force solely on the grounds that the signature on the electronic document is not a handwritten signature;

6.2.2. Distinction between signature levels.

The Bank may use one or all types of Electronic Digital Signature:

a) **A simple electronic signature** is an electronic signature whose signature key matches the electronic signature itself (codes, passwords, and other identifiers) and is used for both internal Bank documents and client documents in any accessible and permitted form, for user authentication.

b) Unqualified Electronic Digital Signature - an electronic signature that is used for documents that do not require the highest level of protection and meets the following criteria:

- obtained as a result of cryptographic transformation of information using a signature key;
- allows you to clearly identify the person who signed the electronic document;
- allows you to detect the fact that changes have been made to an electronic document after it has been signed;
- is created using electronic signature tools that the person who signed the electronic document is able to keep under his or her control.

c) Qualified Electronic Digital Signature - an electronic signature that meets all the characteristics of an unqualified electronic signature and the following additional characteristics:

- the electronic signature verification key is specified in the qualified certificate;
- to create and verify an electronic signature, electronic signature tools that have received confirmation of compliance with the requirements established by the legislation of the Kyrgyz Republic are used.

A qualified electronic digital signature is used to sign legally significant documents, contracts, financial and other reports submitted to authorized government agencies and the National Bank of the Kyrgyz Republic.

6.2.3. Control and audit of use.

a) The Bank shall appoint persons responsible for the issuance, use, recording and control of the use of the Electronic Digital Signature.

b) Regular checks are carried out to check for unauthorized use of the Electronic Digital Signature.

6.2.4. Compatibility, security and integration.

a) The electronic digital signature must be supported by the used Electronic Document Management systems and interact with external services.

b) Compliance with electronic signature standards is ensured for interaction with the Bank's partners/counterparties and government agencies of the Kyrgyz Republic.

c) In the event of compromise, the Electronic Digital Signature must be promptly cancelled and replaced.

6.3. Compliance with these principles enables the effective use of the Electronic Document Management and Electronic Digital Signature systems, ensuring the reliability, security, and legal validity of electronic documents within the Bank.

III. PROCEDURE FOR USE AND SCOPE OF APPLICATION OF ELECTRONIC DOCUMENT MANAGEMENT

7. The Bank uses the Electronic Document Management system, which provides:

- creation, use and storage of electronic documents;
- routing and coordination of electronic documents;
- application of Electronic digital signature;
- interaction with counterparties/clients/partners of the Bank through Electronic Document Management systems that comply with the legislative requirements of the Kyrgyz

Republic.

8. Documents subject to processing in Electronic Document Management include:
   - contracts (including credit, collateral, etc.), agreements, invoices, delivery notes;
   - personnel documents (subject to the relevant consent of employees);
   - internal orders, instructions and memos;
   - other documents that allow electronic form in accordance with the legislation of the Kyrgyz Republic.

9. Access to Electronic Document Management is provided to authorized employees/counterparties/partners/clients of the Bank, as well as, if necessary, to authorized government agencies in accordance with the requirements of the legislation of the Kyrgyz Republic.

10. All participants in the Electronic Document Management System are required to comply with information security requirements and not disclose their login credentials for the Electronic Document Management System.

11. All issues related to the use of Electronic Document Management and the signing of documents using an Electronic Digital Signature are governed by internal regulatory documents that determine the procedure for the operation of Electronic Document Management in the Bank.

IV. PROCEDURE FOR USING AN ELECTRONIC DIGITAL SIGNATURE

12. Obtaining and using an electronic digital signature is carried out in accordance with the legislation of the Kyrgyz Republic.

13. Responsibility for issuing and monitoring the use of Electronic Digital Signatures in the Bank is assigned to the following structural divisions (including, but not limited to):
   - Information security management (establishing security standards or rules, general monitoring of security controls, security audits, risk assessment);
   - IT department (technical support, technical monitoring);
   - Legal Department (control of compliance with the requirements of the legislation of the Kyrgyz Republic).
   - authorized employees and heads of structural divisions.

14. The owner of the Electronic Digital Signature is responsible for the safety of the private key and has no right to transfer it to third parties.

V. SECURITY AND DATA PROTECTION

15. The Bank ensures the protection of information in Electronic Document Management by:
   - use of comprehensive security measures (based on the results of security risk assessment);
   - regular software updates;
   - encryption and data backup.

16. In the event of a compromise of the Electronic Digital Signature, the employee is obliged to immediately notify the responsible person.

17. General control over compliance with security standards and rules when using Electronic Digital Signature is carried out by the Information Security Department.

VI. RESPONSIBILITY AND CONTROL

18. All employees using Electronic Document Management and Electronic Digital Signature are personally responsible for compliance with the Regulation.
19. For violation of the procedure for using the Electronic Digital Signature, disciplinary measures may be applied as provided for by the legislation of the Kyrgyz Republic and the internal regulatory documents of the Bank.
20. Regular checks of compliance with the requirements of the Regulation are carried out:
    - 1st line of defense: Heads of structural and independent divisions of the Bank, IT department ;
    - 2nd line of defense: Information Security Management.
    - 3rd line of defense: The Bank's Internal Audit Service.

VII. FINAL PROVISIONS

21. This Regulation shall enter into force upon approval by the Management Board of the Bank and shall be subject to mandatory execution by all structural divisions of the Bank and officials of the Bank who are participants in the described process.
22. The heads of the Bank's structural divisions are responsible for organizing the timely familiarization, study, application and use of this Regulation by employees.
23. This Policy is subject to revision upon the identification of new vulnerabilities and risks, audit findings, following security incidents, and as needed. All amendments and additions to this Policy are approved by the Management Board after consultation with the Information Security Department.
24. In the event of a conflict between this Regulation and regulatory legal acts, the parties to legal relations shall be guided by the regulatory legal act that has higher legal force.
25. Issues not regulated by this Regulation are governed by the current legislation of the Kyrgyz Republic and regulatory legal acts of the National Bank of the Kyrgyz Republic, decisions of the Board of Directors of the Bank and other internal documents of the Bank.