Privacy Policy for (JB) Mobile Application and Internet Banking Service

1. Who we are?

Company Name: Aljazeera Sudanese Jordanian Bank

Commercial Registration No : 28581

Bank License No. : 11/2008

Registered Address: Africa Street, Khartoum, P.O. Box 424, Khartoum Sudan

Al Jazeera Sudanese Jordanian Bank (hereinafter referred to as "the Bank," "we," or "us"), a licensed banking institution operating in the Republic of Sudan and regulated and supervised by the Central Bank of Sudan (CBOS) ,is committed to protecting the privacy and security of the personal and financial data of its customers and users of the(JB) mobile banking application and Internet Banking service. This Privacy Policy explains the types of data we collect, how we use, share, and protect it, as well as your rights and digital account deletion procedures.

2. Scope of Covered Services

This Policy covers all digital operations and services available via the JB application and Internet Banking, including:

- Digital Account Management :Self-registration and application activation, as well as password and security question resets.
- Inquiries and Statements :Account balance and deposit balance inquiries, financing transaction details, mini-statements (last 5 transactions / last 7 days / last 30 days), historical statements (3 months), and past transaction inquiries.
- Cheque Services :Check-book requests and check status inquiries.
- Fund Transfers :Transfers between the customer's own accounts within the Bank, transfers to other customer accounts within Al Jazeera Sudanese Jordanian Bank, and interbank transfers to other banks via Basic Bank Account Number) BBAN.(
- Payments and Bills :Mobile top-up and bill payments for telecom operators (Zain, Sudani, MTN), electricity token purchases, and government fee payments via the Essaly service).
- Ancillary Services :Managing beneficiary favorites lists and viewing foreign exchange rates.

3. Data We Collect

To deliver the aforementioned services with the highest levels of security and efficiency, the application collects and processes the following categories of data:

- Identity and Verification Data (KYC) :Full name, National ID number, Customer Identification Number (RIM), and mobile phone number registered with the Bank to complete self-registration and identity verification via One-Time Passwords (OTP).
- Financial and Transaction Data :Account and deposit numbers, beneficiary BBANs, cheque details, financing transaction records, and logs of transfers, bill payments, electricity purchases, and Eisali transactions.
- Beneficiary and Payment Lists :Phone numbers, electricity meter numbers, and bill or receipt reference numbers optionally saved by the customer in the Beneficiary Favorites List to facilitate future transactions.
- Security and Authentication Data :Security questions and their encrypted answers, as well as biometric authentication data (fingerprint or facial recognition), which is processed locally on your device's operating system and is never stored on the Bank's servers.

- **Technical and Device Data :**Device model, operating system, Internet Protocol (IP) address, and security session identifiers, used for account protection, fraud prevention, and binding the application to the customer's device.

4. Device Permissions

The **JB** application may request access to certain device features based on your explicit consent to enable specific functionalities:

- **Storage and Files :**To save and download account statements and receipts for transfers, bill payments, electricity purchases, and Essaly Payments.
- **Camera :**To scan Quick Response (QR) codes to facilitate payment and transfer operations.
- **Notifications :**To send real-time alerts regarding executed transactions and security notices.

5. Purposes of Data Use

The Bank uses the collected data exclusively for the following purposes:

- Processing self-registration requests, verifying customer identity, and securing access to the application.
- Processing and executing fund transfers, check book requests, bill payments, electricity purchases, and government fee settlements.
- Personalizing the user experience by maintaining the Beneficiary Favorites List.
- Ensuring full compliance with the regulations and directives of the **Central Bank of Sudan** ,as well as Anti-Money Laundering and Counter-Terrorism Financing (AML/CFT) laws in force in the Republic of Sudan.
- Detecting and preventing suspicious activities, electronic fraud attempts, and safeguarding information security.

6. Data Sharing and Disclosure

Al Jazeera Sudanese Jordanian Bank commits not to sell, rent, or trade your personal or financial data to any third party. Sharing of necessary data to fulfill services is strictly limited to the following entities:

- **Payment Infrastructure Operators :**The National Payment Switch (Electronic Banking Services Co. - EBS) to execute transfers via BBAN, electricity purchase services, and the government electronic collection system (**Essaly).**
- **Telecommunications Service Providers :**Telecom operators (Zain, Sudani, MTN) strictly to the extent required to process airtime top-ups, bill payments, and deliver OTP messages.
- **Regulatory and Judicial Authorities :**The Central Bank of Sudan, the Financial Information Unit (FIU), and competent judicial authorities in the Republic of Sudan whenever required by applicable law.

7. Data Security and Protection

- **Encryption in Transit :**All data transmitted between the **JB** application or Internet Banking browser and the Bank's servers is encrypted using industry-standard cryptographic protocols (**TLS / HTTPS)**.
- **Internal Security Controls :**The Bank enforces advanced security controls, Multi-Factor Authentication (MFA), and encrypted security questions to prevent any unauthorized access to customer accounts.

8. Data Retention

The Bank retains customer information and records collected through its Mobile Banking Application in accordance with applicable laws and regulatory instructions, including the Central Bank of Sudan's record-retention requirements. Relevant customer due diligence records shall be retained for at least five (5) years following termination of the business relationship, while transaction records shall be retained for at least five (5) years from the date of execution or attempted execution of the transaction, as applicable.

9. Account Deletion and Unsubscription Procedures for JB App and Electronic Banking Services

The customer has the right to request the deletion of their **JB** application account and unsubscribe from electronic banking services in accordance with the following rules and procedures:

A. Request Submission Channels:

- **Bank Branches :**Visiting any branch of Al Jazeera Sudanese Jordanian Bank and submitting an account deletion request while presenting a valid proof of identity document.
- **Email :**Sending a request to the Bank's official email address :info@aljazeerabank.com.sd ,using the email address registered within the customer's KYC profile, subject to completing additional identity verification procedures if required.
- **Call Center :**Contacting the unified call center number (**2344**) and submitting an account deletion request after completing customer identity verification procedures in accordance with the Bank's approved controls.

B. Request Processing Procedures:

- The Bank receives the customer's request and verifies their identity and ownership of the account and associated services.
- Upon completion of verification procedures, the customer's subscription to the application is canceled, and login access and use of the digital services associated with the request are terminated.
- The request is processed within **two (2) business days** from the date all verification requirements are fulfilled, subject to the approval of this timeframe by the Bank's competent authorities.
- The customer is notified of the completion of the deletion procedures via their registered contact method.

C. Data Retention Following Account Deletion:

- Deleting the application account or unsubscribing from electronic banking services does not necessarily entail the immediate deletion of all customer data or banking records. The Bank retains data required to be kept under applicable laws, regulations, and regulatory directives—including Anti-Money Laundering and Counter-Terrorism Financing (AML/CFT) requirements—for the legally mandated retention periods.
- Such retained data is kept under strict confidentiality and used solely for legal and regulatory purposes. Upon expiration of the mandated retention periods, the data is deleted or anonymized in accordance with the Bank's approved policies.
- **Important Note :**Requesting the deletion of the application account does not constitute closing the customer's underlying bank account or terminating their banking relationship with the Bank

10. Anti-Money Laundering and Transaction Monitoring

The Bank monitors customer accounts and transactions to detect and prevent money laundering, terrorist financing, fraud and other unlawful activities, in accordance with applicable AML/CFT laws, regulations and regulatory instructions. The Bank may report suspicious activities to the competent authorities as legally required.

11. Customer Consent and Acknowledgment of Privacy Policy

By downloading the **JB** application, accessing the Internet Banking service, registering therein, or continuing to use them, the customer acknowledges that they have read and understood the terms of this Privacy Policy and consents to the collection, processing, use, and disclosure of their personal and financial data in accordance with this Policy and applicable laws and regulatory requirements. Where applicable laws require obtaining explicit consent for specific data processing activities, the Bank commits to obtaining such consent separately.

12. Limitation of Liability

The Bank exercises reasonable care and implements appropriate technical and organizational measures to protect customers' personal data and secure the **JB** application and Internet Banking service. However, the Bank shall not be liable for any losses or damages arising from the customer's misuse of the application, failure to adhere to security instructions, disclosure of login credentials, passwords, security questions, or One-Time Passwords (OTP) to third parties, or events beyond the Bank's reasonable control. Nothing in this clause shall be construed as excluding or limiting the Bank's liability in cases where applicable laws and regulations prohibit such exclusion or limitation.

13. Amendments to the Privacy Policy

The Bank reserves the right to update or amend this Policy from time to time to reflect technical developments or regulatory requirements. Any updates will be published on the Bank's official website and within the application, and your continued use of the service following such updates constitutes acceptance of the revised Policy.

14. Governing Law

This Privacy Policy shall be governed by and construed in accordance with the laws and regulations in force in the **Republic of Sudan** ,and the relevant directives issued by the **Central Bank of Sudan**.

15. Contact Information

For any inquiries regarding this Privacy Policy or data protection, please contact us via:

- **Email:** info@aljazeerabank.com.sd
- **Customer Service Center:** 2344
- **Website:** www.aljazeerabank.com.sd