PRIVACY NOTICE

1. Introduction and Scope

The Reserve Bank of Zimbabwe ("the Bank" or "RBZ") is committed to protecting the privacy, confidentiality and integrity of personal information that it collects, uses, stores, discloses or otherwise processes in the execution of its statutory, regulatory, supervisory, administrative and operational functions.

This Privacy Notice explains how the Bank, acting as a data controller where it determines the purposes and means of processing personal information, processes personal information relating to data subjects who interact with the Bank in any capacity, including regulated institutions, applicants, employees, prospective employees, suppliers, service providers, visitors, complainants, members of the public and users of RBZ websites, portals or other digital platforms.

This notice should be read together with the Bank's Personal Data Protection Policy and any other applicable privacy, information security, records management or data governance policies issued by the Bank from time to time.

2. Personal Information We Process

The Bank shall process personal information in accordance with applicable data protection principles under the Cyber and Data Protection Act [Chapter 12:07], including lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, confidentiality, integrity, security and accountability.

The Bank shall take reasonable steps to ensure that personal information is collected for specified, explicit and legitimate purposes and is not further processed in a manner that is incompatible with those purposes, unless such further processing is authorised by law or otherwise compatible with the Bank's statutory mandate.

3. Personal Information We Process

The nature and extent of personal information processed by the Bank depends on the data subject's relationship with the Bank and the purpose for which the information is required. The Bank may process the following categories of personal information:

- **Identification information:** name, surname, national identity number, passport number, date of birth, identifying symbols or other particulars assigned to a data subject.
- **Contact information:** physical address, postal address, email address, telephone number and related contact details.

- **Financial information:** bank account details, payment records, transaction information, financial history and information submitted in connection with facilities, payments or regulatory reporting.
- **Employment and professional information:** employment history, professional qualifications, fit-and-proper information, board or senior management information, employee records, applicant information and beneficiary details.
- **Regulatory and compliance information:** licensing, registration, supervisory, prudential, enforcement, consumer protection, anti-money laundering, counter-financing of terrorism and related compliance information.
- **Correspondence and opinions:** correspondence submitted to or received from the Bank, including confidential or private communications, complaints, views, opinions or preferences.
- **Technical and online information:** IP addresses, online identifiers, device information, website usage information, cookies and information collected through RBZ websites, portals or mailing lists.
- **Special categories of personal information:** biometric information, CCTV footage, health information, race, gender, marital status, nationality, disability, religion, language, criminal history or other sensitive information, processed only where authorised by law, necessary for a specific lawful purpose, proportionate to that purpose and subject to appropriate safeguards.

4. Purposes and Lawful Bases for Processing Personal Information

The Bank processes personal information where processing is necessary for the performance of its statutory mandate, compliance with legal and regulatory obligations, the performance of public interest functions, the administration of its operations, the protection of its systems and premises, the performance of contractual obligations, the establishment or defence of legal claims, or where consent has been obtained where required by law.

In particular, the Bank may process personal information for the following purposes:

- regulation, licensing, registration, supervision and oversight of banks, microfinance institutions, payment service providers, authorised dealers with limited authority and other financial entities under the Bank's purview;
- prudential supervision, financial stability monitoring, monetary policy implementation, market conduct supervision and consumer protection functions;
- processing applications, approvals, facilities, returns, reports, complaints, investigations, enforcement matters and other regulatory submissions;
- administration of accounts, payments, procurement, contracts, tenders, supplier due diligence and service provider management;
- human resources administration, recruitment, employee management, payroll, benefits, training, security and occupational health matters;
- registration and administration of collateral over movable assets and related statutory or operational processes;
- managing access to RBZ premises, systems, websites, portals, events and mailing lists;
- detecting, preventing and responding to fraud, financial crime, cyber threats, unauthorised access, security incidents or other unlawful activity;
- generating statistical, research, supervisory, economic or policy reports, where appropriate using aggregated or anonymised information; and

- any other purpose that is compatible with the Bank's mandate or authorised by applicable law.

5. Collection of Personal Information

Where reasonable and practicable, the Bank collects personal information directly from the data subject through forms, applications, correspondence, meetings, telephone communications, electronic submissions, websites, portals or in-person interactions.

The Bank may also collect personal information from regulated institutions, appointed agents, employers, service providers, other regulators, public authorities, law enforcement agencies, publicly available sources or other third parties where such collection is lawful and necessary for the Bank's functions.

The Bank may collect information through cookies and similar technologies when a data subject accesses RBZ websites or portals. The Bank may also collect information through security systems, including closed-circuit television facilities and access-control systems at RBZ premises.

6. Use, Disclosure and Transfer of Personal Information

The Bank uses personal information only for lawful, specific and legitimate purposes connected to its mandate and operations. Personal information may be disclosed to third parties where necessary for the Bank's regulatory functions, legal obligations, contractual obligations, security requirements or other lawful purposes.

Such third parties may include other regulators, public authorities, law enforcement agencies, auditors, legal advisers, consultants, service providers, government bodies, international supervisory or financial institutions and other persons or entities authorised by law or contractually engaged by the Bank.

Where personal information is transferred to or processed by third parties, the Bank will take reasonable steps to ensure that appropriate confidentiality, security and data protection safeguards are in place. Where personal information is transferred outside Zimbabwe, such transfer shall only occur where permitted by law and subject to appropriate safeguards, including regulatory cooperation arrangements, contractual protections, adequacy considerations or other legally recognised grounds.

7. Security and Storage of Personal Information

The Bank stores personal information securely and implements appropriate technical and organisational measures designed to protect personal information against unauthorised access, unlawful processing, accidental loss, destruction, alteration or disclosure.

These measures may include access controls, confidentiality obligations, secure storage, information security controls, audit processes, staff awareness and other safeguards appropriate to the nature of the information and the risks associated with its processing.

The Bank shall manage suspected or confirmed personal data breaches, cyber incidents or unauthorised disclosures in accordance with applicable legal requirements, internal incident response procedures and any notification obligations to the Data Protection Authority or affected data subjects, where required by law.

8. Retention of Personal Information

The Bank retains personal information only for as long as is necessary for the purposes for which it was collected or further processed, or as required by applicable law, regulatory requirements, records management rules, contractual obligations, audit requirements, litigation, investigations or the Bank's legitimate operational needs.

The Bank will take reasonable steps to ensure that personal information is adequate, relevant, not excessive, accurate and, where necessary, kept up to date. Personal information that is no longer required will be securely deleted, destroyed, anonymised or archived in accordance with applicable retention requirements.

9. Rights of Data Subjects

Subject to applicable law, lawful limitations and any exemptions recognised under the Cyber and Data Protection Act [Chapter 12:07], data subjects may exercise the following rights in relation to their personal information:

- the right to be informed about the collection and processing of their personal information;
- the right to request access to personal information held by the Bank, subject to applicable procedures and any legally allowable fees;
- the right to request correction or updating of inaccurate, incomplete or outdated personal information;
- the right to request deletion or erasure of personal information where lawful and applicable;
- the right to object to processing or request restriction of processing, where applicable;
- the right to withdraw consent where processing is based on consent, without affecting the lawfulness of processing carried out before withdrawal; and
- the right to lodge a complaint with the Bank or the supervisory authority.

Requests relating to personal information may be submitted to the Data Protection Officer using the contact details set out in this Privacy Notice. The Bank may request information necessary to verify the identity of the requester and to process the request lawfully.

The exercise of data subject rights may be limited where disclosure, deletion, restriction or objection would prejudice the Bank's statutory mandate, supervisory functions, investigations, enforcement processes, financial stability responsibilities, legal privilege, confidentiality obligations or other lawful requirements.

10. Consent and Withdrawal of Consent

The Bank does not rely on consent for all processing activities. In many cases, personal information is processed because it is necessary for the Bank's statutory, regulatory, supervisory, contractual, security or operational functions, or because processing is required or authorised by law. Where the Bank relies on consent as the lawful basis for processing personal information, the data subject may withdraw such consent at any time by contacting the Data Protection Officer. Withdrawal of consent shall not affect the lawfulness of processing carried out before withdrawal, and may affect the Bank's ability to provide certain services, process certain requests or continue a specific interaction where the information is necessary for that purpose.

11. Data Protection Officer

This Privacy Notice is issued by the Reserve Bank of Zimbabwe, 80 Samora Machel Avenue, Harare, Zimbabwe.

Data subjects may contact the Bank's Data Protection Officer regarding privacy-related queries, requests or complaints through the following channels:

- Email: dpo@rbz.co.zw
- Postal or physical address: Reserve Bank of Zimbabwe, 80 Samora Machel Avenue, Harare, Zimbabwe.
- Telephone: 263 242 703000 ext 10101

12. Complaints to the Supervisory Authority

Where a data subject is not satisfied with the Bank's handling of a privacy-related request or complaint, the data subject may lodge a complaint with the Postal and Telecommunications Regulatory Authority of Zimbabwe, which is the designated Data Protection Authority under the Cyber and Data Protection Act [Chapter 12:07].

13. Changes to this Privacy Notice

The Bank may update this Privacy Notice from time to time to reflect changes in law, regulatory requirements, operational practices, technology or the manner in which personal information is processed. Where substantial changes are made, the Bank will take reasonable steps to bring the updated notice to the attention of affected data subjects.

Any amendment will take effect upon publication on the Bank's website at www.rbz.co.zw or through any other appropriate communication channel. Data subjects are encouraged to review the Privacy Notice periodically.

14. Review and Renewal of this Privacy Notice

The Bank shall review this Privacy Notice periodically to ensure that it remains aligned with applicable data protection laws, regulatory requirements, institutional policies, operational practices and changes in the way personal information is collected, used, stored, disclosed or otherwise processed.

The Privacy Notice may be renewed, amended or re-issued where there are material changes in the Bank's processing activities, changes in law or regulation, changes in the Bank's systems or processes, or where a review identifies the need to strengthen privacy, security or data governance arrangements.

The responsibility for coordinating the review and renewal of this Privacy Notice shall rest with the Data Protection Officer, in consultation with relevant departments and subject to approval in accordance with the Bank's internal governance processes.