Global Dot Bank

Banking Beyond Borders

Data Protection & Security Standards

Version 1.0 | Effective: January 2025

1. Objective

To safeguard the confidentiality, integrity, and availability of data within Global Dot Bank through adherence to international information security frameworks.

2. Security Framework

GDB adopts ISO/IEC 27001 and NIST Cybersecurity Framework standards across all information systems.

3. Security Principles

- **Access Control: Role-based and least privilege access model**
- **Encryption: AES-256 for data at rest, TLS 1.3 for data in transit**
- **Network Security: Firewalls, intrusion detection, and zero-trust architecture**
- **Incident Response: Documented plan with escalation within 2 hours of detection**
- **Penetration Testing: Conducted semi-annually by independent third parties**
- **Business Continuity: Redundant data centers across APAC, EMEA, and North America**

4. Vendor Management

All third-party vendors undergo due diligence and security assessment before engagement. Critical vendors must align with GDB's data protection standards.

5. Monitoring & Audit

The Chief Information Security Officer (CISO) oversees continuous monitoring. Quarterly internal audits and annual external reviews are mandatory.

6. Incident Response & Reporting

All breaches are logged and reported to the CISO and the Regulatory Authority within 72 hours. Root-cause analysis and remediation plans are required within 10 business days.

Approved by:
Board of Directors, Global Dot Bank
Date: January 10, 2025