Global Dot Bank

Banking Beyond Borders

# Data Security & Information Governance Manual

*Cybersecurity & Privacy Framework*

### Purpose

To safeguard customer, employee, and institutional data through comprehensive cybersecurity and information governance measures.

### Security Framework

Aligned with ISO 27001, NIST Cybersecurity Framework, and SOC 2 Type II standards.

## 1. Key Policies

### 3.1 Data Classification

- **Confidential: Client data, financials, KYC information**
- **Restricted: Internal correspondence, operational reports**
- **Public: Marketing materials, published financial disclosures**

### 3.2 Access Control

- Role-based access management (RBAC)
- Multi-factor authentication for all privileged accounts
- Automatic session termination after inactivity

### 3.3 Data Encryption

- AES-256 encryption for all sensitive data at rest and in transit
- Secure key management via HSMs
- TLS 1.3 for all communication channels

### 3.4 Network & Endpoint Security

- Continuous monitoring through SIEM and IDS systems
- Annual penetration testing by external cybersecurity auditors
- Patch management SLAs within 72 hours of critical vulnerability disclosure

### 3.5 Incident Response Plan

- 24/7 SOC (Security Operations Center)
- Incident containment, forensic analysis, and post-mortem review
- Regulatory notification protocols within 72 hours (GDPR, PDPA)