Global Dot Bank

INTERNAL USE ONLY - CONFIDENTIAL

Cybersecurity & Technology Governance

Digital Resilience & Information Security Architecture

CONFIDENTIALITY NOTICE

This document contains critical cybersecurity architecture and incident response protocols. Distribution is restricted to CISO, CTO, CRO, Board Risk Committee, and authorized IT security personnel only.

1. Information Security Architecture

1.1 Data Center Infrastructure

- **Tier-4 Certified Data Centers: Singapore, Zurich, Dubai**
- **Geographic Redundancy: Active-active-passive configuration**
- **Physical Security: Biometric access, 24/7 surveillance, mantrap entry**
- **Environmental Controls: N+1 power, cooling, fire suppression**

1.2 Zero-Trust Security Architecture

- **Adaptive Authentication: Multi-factor, risk-based access controls**
- **Hardware Encryption: AES-256 for data at rest, TLS 1.3 for data in transit**
- **Blockchain Transaction Logs: Immutable audit trails for non-repudiation**
- **Automated Incident Detection: AI-powered threat detection and isolation**
- **Network Segmentation: Microsegmentation with east-west traffic inspection**

2. Digital Resilience

2.1 Cyber Fusion Center

A 24/7 Security Operations Center (SOC) monitors all critical systems with real-time threat intelligence integration and automated response capabilities.

2.2 Disaster Recovery Capabilities

Metric	Target	Current Status
Recovery Time Objective (RTO)	< 30 minutes	Validated: 15 minutes
Recovery Point Objective (RPO)	< 5 minutes	Validated: 5 minutes
Failover Testing	Quarterly	Last Test: Pass
Data Backup Frequency	Continuous replication	Active

2.3 Failover Architecture

Automated failover across three redundant data zones in distinct geographi
ensures continuous service availability even during major regional disruptions.

3. Cybersecurity Controls

- Vulnerability Management: Weekly automated scans, monthly penetration tests
- Patch Management: Critical patches deployed within 48 hours
- Access Management: Least privilege principle, quarterly access reviews
- Data Loss Prevention (DLP): Monitoring and blocking of sensitive data exfiltration
- Email Security: Advanced threat protection, DMARC, SPF, DKIM
- Endpoint Detection & Response (EDR): All devices monitored 24/7
- Security Awareness Training: Mandatory quarterly training, phishing simulations

4. Incident Response Protocol

Incident Severity	Response Time	Escalation
Critical (P1)	Immediate	CISO, CEO, Board Chair
High (P2)	< 1 hour	CISO, CRO
Medium (P3)	< 4 hours	Security Team Lead
Low (P4)	< 24 hours	SOC Analyst

4.1 Post-Incident Activities

- Forensic investigation and root cause analysis
- Lessons learned and control enhancement
- Regulatory notification (if required)
- Customer communication (if data breach)
- Board and management briefing

Critical Cyber Incident Protocol

Any incident involving data breach (>100 customers), system compromise, or ransomware requires immediate activation of Crisis Management Committee (CMC) and notification to Board Chair within 2 hours. External cyber forensics firm engagement mandatory for P1 incidents.