FINANCIAL MARKETS DIVISION

NATIONAL PAYMENT SYSTEMS DEPARTMENT (NPSD)

Guidelines on Digital Financial Services (DFS) Security in Zimbabwe

JULY 2026

Table of Contents

LIST OF ACRONYMS

Acronym	Full Name
AES	Advanced Encryption Standard
API	Application Programming Interface
APK	Android Package (application file format for Android OS)
CEH	Certified Ethical Hacker
CERT	Computer Emergency Response Team
CISSP	Certified Information Systems Security Professional
CISO	Chief Information Security Officer
CSIRT	Computer Security Incident Response Team
DFS	Digital Financial Services
DDoS	Distributed Denial of Service
DevSecOps	Development, Security, and Operations
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IOC	Indicator of Compromise
IP	Internet Protocol
ISO	International Organization for Standardization
ITU	International Telecommunication Union

KYC	Know Your Customer
MFA	Multi-Factor Authentication
mPOS	Mobile Point of Sale
OTP	One-Time Password
PIN	Personal Identification Number
PSP	Payment Service Provider
RBZ	Reserve Bank of Zimbabwe
SLA	Service Level Agreement
SIM	Subscriber Identity Module
SAST	Static Application Security Testing
SS7	Signalling System No. 7 (telecom signaling protocol)
TLS	Transport Layer Security
TEE	Trusted Execution Environment
USSD	Unstructured Supplementary Service Data
WAF	Web Application Firewall

DEFINITION OF TERMS

Term	Definition
Digital Financial Services (DFS)	Financial services accessed and delivered through digital channels, such as mobile phones, internet, ATMs, POS devices, and agent banking platforms.
Rooted/Jailbroken Device	A digital device whose operating system security restrictions have been bypassed, increasing its vulnerability to malware and unauthorized control.
SIM Swap Fraud	A type of fraud in which a malicious actor gains control of a user's phone number by tricking a telecom provider into issuing a new SIM tied to that number.
SS7 Vulnerability	Security flaws in the Signaling System 7 (SS7) telecom protocol that allow attackers to intercept calls, SMS, and bypass two-factor authentication.
Biometric Authentication	Verification of identity based on biological characteristics such as fingerprint, facial features, or iris scan and voice recognition.
Multi-Factor Authentication (MFA)	An authentication method requiring two or more verification factors, such as PIN + fingerprint or password + OTP.
Penetration Testing	A simulated cyberattack used to evaluate the security of a system by identifying exploitable vulnerabilities.
Device Fingerprinting	A technique to uniquely identify a device based on its hardware and software characteristics, often used for fraud detection.
Zero-Trust Architecture	A security model that assumes no trust by default, even inside the network, requiring continuous authentication and strict access controls.
Incident Response Plan	A structured approach outlining how an organization detects, responds to, and recovers from cybersecurity incidents.

Encryption	The process of converting data into a coded format to prevent unauthorized access.
Threat Intelligence	Information about potential or current attacks gathered and analysed to help prevent or mitigate cybersecurity threats.
Data Residency	A legal and regulatory requirement for data to be stored in a specific geographic location or jurisdiction.

1. INTRODUCTION

1.1 This guideline establishes the minimum-technical security requirements for safeguarding Digital Financial Services (DFS) in Zimbabwe.

1.2 The DFS Technical Security Guideline draws on the global best practices, particularly the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) recommendations and contextualises these for the unique cybersecurity threats facing mobile- and internet-enabled financial ecosystems. Its scope is sector-specific and complementary to the Reserve Bank of Zimbabwe's Cybersecurity and Resilience Guideline of August 2025, which serves as the overarching cybersecurity framework for regulated institutions.

2. OBJECTIVES OF THE GUIDELINE

2.1 Strengthen the resilience of DFS platforms against known and emerging digital threats.

2.2 Promote secure digital financial inclusion.

2.3 Define a risk-based approach to security across DFS components: end-user devices, access channels, applications, and backend systems.

2.4 Clarify regulatory expectations and escalation procedures in the event of DFS-related incidents.

3. SCOPE AND APPLICABILITY

The guideline applies to the following DFS ecosystem entities operating in Zimbabwe:

3.1 All RBZ-licensed institutions, which offer digital financial services, including financial institutions (banks and microfinance institutions etc), mobile money operators, fintechs, and payment service providers (PSPs).

3.2 DFS intermediaries such as Aggregators, DFS agents, and third-party service providers who operate within or interface with DFS platforms.

3.3 These guidelines exclude telecom infrastructure-level controls such as mobile base stations, among others.

3.4 Where integration with telecom networks occurs, that is for USSD/SMS, DFS providers must mitigate known vulnerabilities, including SS7-based attacks, as part of shared risk management.

4. GOVERNANCE AND STRATEGIC RISK MANAGEMENT

4.1 Information Security Governance

- All DFS providers must operate within the enterprise-wide cybersecurity governance framework established under the Reserve Bank Cybersecurity and Resilience Guideline (August 2025), Section 3. The enterprise Chief Information Security Officer (CISO) or equivalent officer accountable for information security shall have oversight of DFS security. DFS providers must additionally appoint a DFS Security Lead responsible for the DFS-specific threat landscape and for coordinating with the enterprise CISO on DFS-related risks. The framework must:

a) Align with the international standards referenced in the Cybersecurity and Resilience Guideline (August 2025) (Section 3.23), including ISO/IEC 27001, the NIST Cybersecurity Framework, and ITU DFS Security Guidelines.

b) Integrate DFS-specific threat models across devices, applications, network, and backend layers.

c) Clearly define internal security policies, escalation paths, and incident communication protocols.

d) Include zero-trust principles, requiring continuous verification of device, user, and network trust before granting access to DFS systems.

e) Explicitly cover controls for mobile device integrity, SIM swap fraud, SS7 vulnerabilities, customer authentication, and backend system protection.

4.2 DFS Threat Risk Assessments

- DFS providers shall conduct formal risk assessments at least annually, or whenever significant changes occur in their service delivery model, infrastructure, or threat landscape. These assessments must adopt a layered risk perspective, including:

a) Device-Level Threats: Rooted/jailbroken devices, mobile malware, keyloggers, and USSD injection.
b) Application-Level Risks: Code tampering, fake apps, insecure downloads, and lack of application vetting.
c) Network and Channel Threats: Exposure to SS7 signaling vulnerabilities, SIM swap fraud vectors, SMS OTP interception, unsecured USSD/SMS sessions.
d) Customer Authentication Risks: Insecure credentials, predictable PINs, weak fallback recovery processes.
e) Backend Threats: Cloud misconfiguration, inadequate firewalls, lack of real-time monitoring.
f) All risk assessments must be documented and submitted to RBZ upon request. DFS providers must demonstrate active mitigation planning and tracking against assessed risks.

5. MOBILE DEVICE AND APPLICATION SECURITY

5.1 Mobile Device Integrity

- DFS providers must implement controls to prevent access from compromised or high-risk devices and ensure the security of client-side environments. Minimum requirements include:

a) Detection and blocking of rooted/jailbroken devices, using device integrity checks, i.e. SafetyNet or equivalent.
b) Deployment of runtime protection against:
   i. Keylogging tools
   ii. Screen capture malware

iii. Overlay attacks such as fake login overlays, among others.

c) Prevention of unauthorised USSD injections by validating session requests and implementing USSD encryption where possible.

d) Prohibition of unencrypted storage of PINs, session tokens, or sensitive user data on client devices or local caches.

e) DFS apps should regularly validate device compliance during logins and restrict high-risk actions on compromised devices.

5.2 DFS Application Integrity

- DFS applications must be protected from tampering, reverse engineering, and unauthorised duplication. At a minimum, providers shall:

a) Apply code obfuscation, anti-debugging, and anti-repackaging techniques in mobile apps.

b) Enforce use of digitally signed and validated code using secure code signing certificates.

c) Verify hash integrity of application packages (APK/iOS builds) during updates and rollout.

d) Maintain a secure DevSecOps pipeline with static and dynamic application security testing (SAST/DAST) before release.

e) Application vetting and post-market monitoring must be instituted to detect rogue clones and fake DFS apps in app stores.

f) Enforce app store take-down SLAs for rogue apps.

g) Mandate rapid revoke/rollback of tainted releases.

h) Require signed Software Bill of Materials (SBOM) and verified build provenance.

5.3 SIM and SS7-related Controls

- DFS providers must recognise and mitigate threats emanating from insecure mobile telecom protocols, particularly Signalling System 7 (SS7) and SIM vulnerabilities. Requirements include:

a) Educate internal teams on SS7 exploits that allow interception of SMS-based OTPs, location tracking, and call/SMS hijacking.
b) Promote token-based or app-based multi-factor authentication (MFA) over SMS OTPs, especially for high-value or high-risk transactions.
c) Integrate SIM swap fraud detection mechanisms into onboarding and login flows, including:
   i. Real-time alerts of SIM changes.
   ii. Velocity checks on credential resets post-SIM change.
   iii. Mandatory customer re-authentication (biometric or alternate channel verification) before reactivating dormant accounts on new SIMs.
   iv. Enforce 24- 48 hour hold windows after SIM change for limit increases or recovery.
   v. require number-recycling checks.
   vi. Define API hooks to ingest MNO SIM swap/port/recycle signals when available.

6. CONSUMER PROTECTION AND AUTHENTICATION

DFS providers must implement robust, multi-layered authentication and user onboarding processes that are resistant to impersonation, credential theft, and device spoofing.

6.1 Secure Customer Onboarding and Access

a) Biometric Authentication: Encourage use of biometric authentication (fingerprint, facial recognition etc.) for supported devices, especially for transaction approval and login, while ensuring fallback options are equally secure.
b) User-Defined PINs and Secrets; users must create their own PINs, which should be protected from:
   i. Shoulder surfing via obscured entry (masked PIN input).
   ii. Display capture or overlay attacks via application hardening.
   iii. Brute-force attacks via retry limits and temporary account lockout.
c) Session Security, DFS platforms must enforce:

i. Automatic session termination after a period of inactivity (default timeout: 3–5 minutes)
ii. Logout mechanisms after high-risk actions such as change of device, SIM swap detection among others.

d) Device Binding and Trust Models; DFS applications must associate trusted user devices through device fingerprinting, with secure procedures to register, deregister, or change trusted devices.

6.2 Protection from Social Engineering and Fraud

- DFS providers must proactively address social engineering threats, including phishing, vishing, SIM swap scams, and fake DFS support agents. Providers must:

a) Deploy behavioral analytics systems that detect:
i. Login attempts from unfamiliar devices, geographies, or networks.
ii. Unusual transaction patterns immediately following credential changes.
iii. Inconsistent device/browser characteristics.

b) Adopt user alerting mechanisms. Notify users immediately of:
i. SIM card changes
ii. New device access
iii. Failed login attempts or account recovery actions

c) Adopt customer support protocols. Call centre and branch staff must:
i. Verify device history and user identity before executing high-risk account changes such as PIN reset, device switch among others.
ii. Use secure challenge-response protocols, not static security questions alone.

d) User Education and Digital Hygiene. DFS providers must regularly communicate:
i. Safe usage practices.
ii. Indicators of fraud or impersonation.
iii. Steps to report suspicious activities.

7. DATA SECURITY AND PLATFORM PROTECTION

7.1 Data Confidentiality and Integrity

- DFS providers must ensure that all customer data is protected throughout its lifecycle- at rest, in transit, and during processing. The following minimum requirements apply:

a) Data Encryption Standards:

i. All sensitive customer data must be encrypted in accordance with the cryptographic standards mandated in the Reserve Bank Cybersecurity and Resilience Guideline (August 2025) (Section 4.10). At minimum, AES-256 or equivalent strength shall be applied. DFS-specific implementations must additionally ensure encryption within secure enclaves and TEEs on mobile devices.

ii. Encrypted channels such as TLS 1.2 or higher must be used for all data transmissions, consistent with the Cybersecurity and Resilience Guideline (August 2025) (Section 4.10).

b) Secure Application Behaviour:

i. DFS applications must disable screen capture functions (via OS-level flags).

ii. Prevent app-switch screenshotting or overlay exploits that could leak data.

iii. Automatically clear the clipboard and cache memory following data entry.

c) Tamper-Resistant Storage:

i. PINs, tokens, and sensitive identifiers must never be stored in plain text on local devices or browsers.

ii. Use Secure Enclaves or Trusted Execution Environments (TEEs), where supported, for storing sensitive credentials.

7.2 Backend and Cloud Infrastructure

- All DFS back-office systems and cloud-hosted platforms must adopt a multi-layered security architecture and enable continuous monitoring. Requirements include:

a) Web and Application Layer Protection:

(refer to Cybersecurity and Resilience Guideline (August 2025), Section 4.9 for enterprise-wide network security requirements):

i. Implement Web Application Firewalls (WAFs) with DFS-specific rulesets to defend against injection attacks targeting mobile APIs, USSD gateways, and web-based DFS portals.

ii. Deploy Intrusion Detection/Prevention Systems (IDS/IPS) as mandated in the Cybersecurity and Resilience Guideline (August 2025) (Section 4.9), with additional DFS-specific detection signatures for mobile transaction anomalies.

iii. Ensure DFS platform resilience against Distributed Denial of Service (DDoS) attacks using throttling, filtering, and traffic scrubbing mechanisms, with specific focus on USSD and API gateway availability.

b) Cloud Security and Data Residency; For DFS providers leveraging cloud services:

i. Data residency must comply with RBZ-defined jurisdictional requirements.

ii. Logs, backups, and audit trails must remain accessible to RBZ upon request.

iii. Cloud configurations must follow zero-trust principles, including least privilege access, network segmentation, and hardened virtual machines.

c) System Hardening and Patch Management:

(refer to Cybersecurity and Resilience Guideline (August 2025), Sections 4.11–4.12 for the enterprise change and patch management framework):

i. Apply routine patching of all DFS systems, applications, and middleware in accordance with the formal change management process established under the Cybersecurity and Resilience Guideline (August 2025). All changes to DFS production environments must follow the four-eyes approval principle and include rollback procedures.

ii. Disable unused ports, services, and default admin accounts on production servers.

8. MONITORING, DETECTION, AND INCIDENT RESPONSE

8.1 Real-time Monitoring and Anomaly Detection

- DFS providers must maintain robust real-time monitoring systems capable of detecting unusual behavior, emerging threats, and security breaches across all service layers. Minimum technical requirements include:

a) Device and User Fingerprinting

i. Generate unique digital fingerprints for user devices and correlate with login activity, transaction origin, and geo-behavioral patterns.

b) Velocity and Behavioral Analytics

- Monitor transactional velocity to detect fraud patterns such as:

i. Sudden spikes in transfers

ii. Multiple rapid credential recovery attempts

iii. Transactions from unfamiliar geographies or after SIM changes

c) Geo-Location and SIM Change Alerts. Implement alerts for:

i. Device access from geographically distinct IPs

ii. Transactions shortly after SIM card changes

iii. Access from high-risk proxies or anonymizers

8.2 Incident Reporting and Forensics

- DFS operators must establish documented protocols for incident response, including clear communication lines with RBZ and internal escalation paths.

a) Mandatory Incident Response Procedures:

- Report any confirmed or suspected compromise, whether technical or fraud-related to RBZ via designated channels. For example, fraud, platform downtime, customer data compromise, among others, must be reported within 3 hours in line with the Cybersecurity and Resilience Guideline of August 2025, Section 8.11).
- Reports must include:

i. Attack vector (i.e. SS7-based OTP hijack, SIM swap, APK injection).

ii. Scope of compromise (affected users/systems).

iii. Initial root cause analysis and containment measures taken.

iv. Preliminary impact assessment.

b) Forensic Evidence Retention

- Maintain:

i. Immutable security logs for all DFS activities (including logs of privileged access).

ii. At least five (5) years of archived logs for incident investigation and regulatory audit.

iii. Tools to reconstruct session flows and identify command injection or unauthorized access paths.

c) Quarterly Reporting

- Submit quarterly breach and risk exposure summaries to RBZ, highlighting:

i. Detected threats

ii. False positives

iii. Actionable insights or control gaps

8.3 Business Continuity and Disaster Recovery for DFS Platforms

i. In accordance with the Cybersecurity and Resilience Guideline (August 2025) (Sections 4.24–4.40), DFS providers must establish and maintain formal Business Continuity Plans (BCP) and Disaster Recovery (DR) procedures specific to their digital financial services. The following minimum requirements apply:

ii. a) Define Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for all critical DFS platforms, including mobile money systems, USSD channels, and API gateways.

iii. b) Conduct regular DR testing, including failover to alternate sites, at least annually or following significant infrastructure changes.

iv. c) Ensure that BCP/DR plans address DFS-specific scenarios such as mass SIM swap events, mobile platform outages, and payment gateway failures.

9. AGENT AND THIRD-PARTY SECURITY

DFS agents and third-party service providers form an essential component of Zimbabwe's digital financial services ecosystem. Given their exposure to operational,

fraud, and endpoint risks, the following minimum controls must be implemented. In addition to agent and vendor controls, DFS providers must apply the Human Resources security lifecycle controls mandated in the Cybersecurity and Resilience Guideline (August 2025) (Sections 4.13–4.17) to all internal personnel with access to DFS backend systems. This includes pre-employment background screening, ongoing access reviews, and immediate credential revocation upon termination.

9.1 **Agent Endpoint and Transaction Security**

- DFS providers shall ensure that their agents operate using secured, auditable, and RBZ-compliant environments. Minimum security measures include:

a) Secure Device Standards
   i. Agents must use industry-approved mobile point-of-sale (mPOS) devices, hardened Android smartphones, or secure USSD-enabled feature phones configured solely for DFS operations.
   ii. Devices must support secure PIN entry, session timeouts, and have up-to-date security patches.

b) SIM and Handset Management; Agents must:
   i. Immediately report lost, stolen, or compromised handsets or SIM cards.
   ii. Use SIMs with two-factor binding to agent identity or business registration.
   iii. Avoid use of dual-SIM devices for DFS operations unless securely containerized.

c) Agent Authentication and Audit Trails
   i. DFS systems must enforce unique login credentials for each agent, prohibit password sharing, and capture full agent activity logs.
   ii. Time-stamped digital receipts and geo-tagged transaction logs must be maintained for auditability.

9.2 Third-Party Integrations and Vendor Risk Management

- All third-party applications, APIs, middleware platforms, and white-labeled DFS tools must undergo rigorous vetting and certification before onboarding. Requirements include:

a) Penetration Testing and Code Review

i. All third-party solutions must undergo penetration testing and code review, either internally or through RBZ-approved cybersecurity firms.

ii. Providers must submit vulnerability remediation plans for any high-risk findings before launch.

b) Security and SLA Clauses

Refer to Reserve Bank Cybersecurity and Resilience Guideline (August 2025), Section 5 for the comprehensive third-party risk management framework:

i. DFS providers must include information security, breach notification, and data protection clauses in contracts with vendors and integrators, consistent with the contractual safeguards mandated in the Cybersecurity and Resilience Guideline (August 2025) (Section 5.5–5.6). DFS-specific contracts must additionally address API security standards, mobile app white-label certification, and agent device vetting.

ii. Providers must obtain Service Level Agreements (SLAs) with clear security Key Performance Indicators (KPIs).

c) API and Data Exchange Security; APIs must:

i. Use OAuth 2.0, mTLS, or equivalent secure access tokens.

ii. Be rate-limited, monitored, and version-controlled.

iii. Prohibit excessive data exposure and allow only least-privilege data access.

10. REGULATORY OVERSIGHT

The Reserve Bank of Zimbabwe (RBZ), as the designated DFS regulator, shall maintain a proactive supervisory role over the cybersecurity posture of DFS providers. This will include continuous assessments, audits, and issuance of timely advisories in response to emerging digital threats.

10.1 Supervisory Activities

- RBZ will conduct the following oversight functions:

a) Check for Security Audits and Penetration Testing

i. Review independent penetration tests and vulnerability scans on DFS platforms (especially high-risk channels such as USSD, mobile apps, and APIs).

ii. Review third-party red-teaming exercises to simulate real-world attacks and assess response readiness.

iii. DFS providers handling critical payment infrastructure must additionally implement Threat-Led Penetration Testing (TLPT) programmes, as mandated in the Cybersecurity and Resilience Guideline (August 2025) (Sections 4.41–4.58), targeting DFS-specific attack surfaces including mobile applications, USSD channels, and agent endpoints.

b) On-site and Remote Inspections; RBZ reserves the right to:

i. Conduct routine and ad hoc inspections.

ii. Review digital logs, incident reports, access controls, and data encryption standards.

iii. Interview CISOs and technical teams as part of compliance reviews.

c) Thematic Reviews; RBZ will carry out reviews focusing on priority risks such as:

i. SS7 vulnerability exposure.

ii. SIM swap fraud incidence.

iii. Mobile app security maturity.

iv. Cloud infrastructure protection.

10.2 Reporting Requirements by DFS Providers

- DFS providers must adhere to the following mandatory reporting obligations:

a) Annual Cybersecurity Audit Reports: Submit comprehensive cybersecurity audit reports conducted by certified cybersecurity firms, aligned with RBZ standards and ITU security benchmarks.

- Reports must include:

i. Audit scope and tools used

ii. Identified vulnerabilities and severity ratings

iii. Mitigation and remediation timelines

b) Breach and Exposure Reports: Submit reports detailing:

i. Detected cyber incidents or fraud cases

ii. Internal security breaches

iii. Risk exposures under monitoring

iv. System changes affecting the security posture (i.e. app rebuilds, cloud migration)

c) Immediate Escalations

i. Major incidents (i.e. customer data compromise, mass fraud, platform downtime) must be escalated urgently, within 3 hours, accompanied by interim incident analysis and containment status.

11. CAPACITY BUILDING AND SECTOR COORDINATION

To strengthen the overall resilience of Zimbabwe's DFS ecosystem, RBZ shall promote continuous capacity development and collaborative threat intelligence sharing across DFS providers, agents, and technical vendors. In addition to the enterprise-wide cybersecurity training programme mandated under the Cybersecurity and Resilience Guideline (August 2025) (Section 7), RBZ shall promote DFS-specific capacity development and collaborative threat sharing across DFS providers, agents, and technical vendors.

11.1 Sector-Wide CERT/CSIRT Collaboration

- RBZ will support the establishment and operationalisation of a Digital Finance–Specific Computer Emergency Response Team (DFS-CERT) or facilitate collaboration through existing national CSIRT frameworks. Responsibilities include:

a) Threat Intelligence Sharing

i. Facilitate sharing of Indicators of Compromise (IOCs), malware signatures, phishing campaigns, and fraud tactics targeting DFS platforms.

ii. Promote joint response to sector-wide incidents (i.e. SS7 breach, malware outbreak, zero-day exploits).

b) Simulated Incident Response Exercises; Conduct regular tabletop exercises with DFS providers to test:

i. Crisis coordination
ii. Incident communication
iii. Recovery and forensic readiness

c) Early Warning Systems

i. Collaborate on threat feed aggregation tools and dashboards to enable proactive detection and sector-wide alerts.

11.2 DFS-Focused Cybersecurity Training and Certification

- RBZ will work with partners to promote specialised cybersecurity training targeted at DFS stakeholders. Key initiatives include:

a) For DFS Operators, regular training on:

i. Secure app development (DevSecOps).
ii. Threat modeling.
iii. Incident response planning.
iv. Fraud analytics and behavioral monitoring.

b) For DFS Agents, practical guidance on:

i. Safe mobile device use.
ii. Recognising social engineering threats.
iii. Reporting and escalation procedures for device compromise or fraud suspicion.

c) For Technical Vendors

i. Encourage vendor participation in RBZ-led technical roundtables, sandbox discussions, and secure integration workshops.

d) Certification Encouragement

i. Promote staff certification in cybersecurity domains such as:
ii. Certified Information Systems Security Professional (CISSP).

iii. Certified Ethical Hacker (CEH).

iv. Mobile App Security certifications (i.e. Android ATC).

12. COMPLIANCE AND SANCTIONS

All DFS providers, agents, and third-party service partners must ensure full compliance with the provisions outlined in this guideline. Non-compliance may result in regulatory action based on the severity, frequency, and risk impact of the violation. Non-compliance may result in:

12.1 Compliance Monitoring

- RBZ shall monitor compliance through:
  i. Scheduled and surprise audits
  ii. Review of periodic reports (breach logs, audit outcomes, risk registers)
  iii. Incident analysis reports following any DFS-related breach or fraud
  iv. Inspection of third-party contracts and technical integrations
- Where providers demonstrate material gaps, RBZ may issue written directives outlining mandatory remediation timelines and follow-up verification requirements.

12.2 Enforcement Actions and Penalties

Depending on the nature of the breach or violation, RBZ may apply the following measures:

Breach Severity	Examples	Potential Sanctions
Minor	Delayed reporting, partial audit gaps.	Formal caution or improvement notice.
Moderate	Repeat failure to implement known security patches or risk assessments.	Monetary penalties, mandatory third-party audit.
Severe	Data breach, customer fraud due to negligence, failure to report within 3hrs	Suspension of services, rollback of product launches, or license revocation.

- The RBZ reserves the right to publish names of sanctioned providers for transparency and deterrence.

12.3 **Remediation and Support**

- RBZ shall provide remediation support where feasible, this may include:
  i. Technical guidance or sandboxing for secure rebuilds
  ii. Referrals to pre-qualified cybersecurity firms
  iii. Conditional timelines for staged compliance

13. EFFECTIVE DATE OF OPERATION

These Guidelines shall take effect from 17 July 2026.

14. APPROVAL OF THE GUIDELINES

The Reserve Bank of Zimbabwe official's signature placed hereinunder certifies the approval of these Guidelines.

Dr. J. Mutepfa

Deputy Director

Financial Market Division -National Payment Systems

RESERVE BANK OF ZIMBABWE

HARARE

17 July 2026

Headquarters:
80 Samora Machel Avenue, Box 1283, Harare, Zimbabwe.
Tel: +2638677000477, +263242703000
Regional Branch:
93 Leopold Takawira Avenue, Box 399 Bulawayo, Zimbabwe.
Tel: +2638677002046, +26329272141-5

communications@rbz.co.zw
www.rbz.co.zw
@ReserveBankZim
@ReserveBankZim