# Security Policy for Fundi Technology (Pty) Ltd t/a www.topitup.io

**Last Updated:** July 18, 2025

Topitup.io takes security seriously. We use industry-standard measures to protect your transactions and account information, ensuring the integrity, confidentiality, and availability of our digital assets and your personal information. This policy outlines our commitment to POPIA's "Security Safeguards" condition.

## 1. Core Security Measures and Compliance

1.1. Data Protection Principles:

1.1.1 Encryption: We implement robust encryption protocols for sensitive data, both at rest (stored data) and in transit (data being transmitted). This includes the use of strong encryption standards like AES-256. Our website uses secure HTTPS (TLS) for all pages, encrypting all data transmitted between your browser and our servers.

1.1.2 Access Controls: We enforce strict access control policies based on the principle of least privilege, ensuring that employees and systems only have access to the data and resources necessary for their specific roles. Multi-Factor Authentication (MFA) is deployed for all critical systems and user accounts. Role-Based Access Control (RBAC) is utilized to manage permissions efficiently.

1.1.3 Audit Trails: We maintain comprehensive and regularly reviewed audit logs for all system access and data handling activities. These logs are crucial for detecting suspicious behavior, investigating incidents, and demonstrating compliance.

1.1.4 Patch Management: We establish a rigorous and timely patch management program to ensure that all operating systems, applications, and network devices are regularly updated with the latest security patches. Proactive patching is vital to prevent exploits and fulfill POPIA's requirement for adequate data protection.

1.2. Risk Management:

1.2.1 Regular Risk Assessments: We conduct periodic and thorough risk assessments to identify internal and external vulnerabilities and threats to personal data and system integrity, as mandated by POPIA Section 19.

1.3 Vulnerability Assessments and Penetration Testing: We implement a schedule for

regular vulnerability assessments and penetration testing. These tests simulate real-world attacks to identify weaknesses in systems, applications, and networks before malicious actors can exploit them.

## 2. Incident Response and Breach Notification Plan

2.1. **Legal Obligation:** Fundi Technology (Pty) Ltd is legally obligated under POPIA to notify the Information Regulator and affected data subjects "as soon as reasonably possible" after becoming aware of a data breach. Where feasible, notification to the Regulator should be no later than 72 hours.

2.2. **Notification Content:** Notifications will be in writing and include: a description of the breach, its likely consequences, measures taken or intended to address it, recommendations for data subjects to mitigate effects, and the identity of the unauthorized party if known.

2.3. **Communication Methods:** Permissible communication methods for breach notifications include post, email, prominent website placement, or news media publication.

2.4. **Internal Procedures:** We have detailed internal incident response procedures, including clear roles and responsibilities for a data breach team, communication protocols, and the process for preliminary assessment, containment, recovery, and detailed investigation. Regular practice breach simulations are conducted to test and refine these procedures.

## 3. Employee Security Awareness Training

3.1. We acknowledge that human error is a significant factor in cybersecurity incidents. Therefore, employee training is a critical defense mechanism, empowering staff to recognize and effectively respond to cyber threats.

3.2. We implement tailored training programs covering cybersecurity best practices, identification of phishing attempts (including SMS and voice phishing), social engineering tactics, and secure data handling. Realistic phishing simulations are conducted to test and improve employee awareness and response capabilities.

3.3. We foster a strong, security-conscious culture within the organization, promoting vigilance and responsible behavior among all employees.

## 4. Data Backup and Disaster Recovery

We establish comprehensive data backup strategies, ensuring that critical systems and data are regularly backed up, encrypted, and stored in secure, offsite locations. We develop and regularly test a disaster recovery and business continuity plan to minimize downtime and ensure the prompt restoration of services and data in the event of an incident.

## 5. Payment Security Standards

5.1. **Payment Gateways:** We process payments via Ozow (Instant EFT) and PayFast (by Network), both of which are licensed and PCI-DSS Level 1 compliant. These platforms encrypt all payment data end-to-end. Your bank account or card details are never exposed to us.

5.2. **3D Secure Implementation:** As mandated by the Payment Association of South Africa (PASA), we implement 3D Secure for all card-not-present e-commerce transactions to enhance security and reduce fraud.

## 6. Recommended Security Audit and Penetration Testing Frequencies

| Type of Assessment | Recommended Frequency | Rationale/Compliance Driver |
|---|---|---|
| **Vulnerability Assessment** | At least Quarterly | Continuous identification of weaknesses, rapid adaptation to evolving threats |

| | | |
|---|---|---|
| **External Penetration Test** | At least Annually | PCI DSS requirement, POPIA Section 19, baseline security check |
| **Internal Penetration Test** | Annually or after major internal changes | Assess internal network security, insider threat mitigation |
| **Web Application Penetration Test** | Bi-annual or Quarterly (for high-risk apps) | Critical for e-commerce platforms handling sensitive data, frequent changes |
| **API Penetration Test** | Bi-annual or Quarterly (if APIs are core to service) | Essential for securing data exchange between systems, especially with third-party integrations |
| **Security Audit / Compliance Audit** | Regularly, or as mandated by regulations | Assess compliance posture, identify gaps, demonstrate due diligence |
| **Event-Driven Testing** | On-demand (after significant infrastructure changes, security incidents, new threats) | Immediate response to new vulnerabilities or changes that could introduce risk |