Afrivest Capital Cybersecurity Policy

Author: Kagiso Pila

Next Review: December 2026

1. PURPOSE

This Cybersecurity Policy establishes the framework for protecting Afrivest Capital (Pty) Ltd's information systems, digital infrastructure, and client data against cyber threats, in line with FSCA CASP requirements and industry best practices.

2. SCOPE

This policy applies to all employees, contractors, systems, networks, and third-party service providers interacting with Afrivest's IT environment.

3. REGULATORY FRAMEWORK

Afrivest adheres to applicable South African regulations including FAIS, FSCA CASP requirements, POPIA, and cybersecurity best practices such as ISO/IEC 27001.

4. GOVERNANCE AND RESPONSIBILITIES

Key Individual, and Compliance Officer oversee cybersecurity governance.

IT personnel are responsible for implementation and monitoring of controls.

5. RISK MANAGEMENT

Afrivest conducts regular cybersecurity risk assessments to identify, evaluate, and mitigate risks. A risk register is maintained and updated periodically.

6. ACCESS CONTROL

Access to systems is restricted based on role and least privilege principles. Multi-factor authentication (MFA) is enforced for critical systems.

7. DATA PROTECTION

Sensitive data is encrypted both in transit and at rest. Client information is handled in compliance with POPIA requirements.

8. NETWORK SECURITY

Afrivest employs firewalls, intrusion detection/prevention systems, and secure network configurations to protect against unauthorized access.

9. CRYPTO ASSET SECURITY

Crypto assets are secured using cold storage, multi-signature wallets, and strict key management protocols.

10. INCIDENT RESPONSE

Afrivest maintains an incident response plan to detect, respond to, and recover from cybersecurity incidents. Incidents are reported to relevant authorities where required.

11. MONITORING AND LOGGING

Continuous monitoring and logging of systems are implemented to detect suspicious activities and ensure audit trails.

12. THIRD-PARTY RISK MANAGEMENT

Afrivest conducts due diligence on all third-party service providers and ensures contractual cybersecurity obligations are in place.

13. EMPLOYEE AWARENESS

Regular cybersecurity training is provided to employees, including phishing awareness and secure handling of data.

14. BUSINESS CONTINUITY

Disaster recovery and business continuity plans are in place to ensure operational resilience in the event of a cyber incident.

15. POLICY BREACHES

Any breaches of this policy must be reported immediately and may result in disciplinary action.

16. REVIEW AND UPDATES

This policy is reviewed annually or upon significant changes in the threat landscape or regulatory requirements.