

RuraRide Security Policy

1. Introduction

At **RuraRide (Pty) Ltd**, we take the security of our users, partners, and systems seriously.

This Security Policy outlines the measures we have implemented to ensure that all personal data, payment information, and digital interactions are protected against unauthorized access, misuse, alteration, or loss.

RuraRide complies with the **Protection of Personal Information Act (POPIA)**, **Cybercrimes Act (No. 19 of 2020)**, and global standards for data security, including the **Payment Card Industry Data Security Standard (PCI DSS)**, through our trusted payment gateway partners such as **PayFast**.

2. Scope

This policy applies to:

- All RuraRide systems, including mobile applications, websites, and cloud-based services.
 - All users (riders and drivers), employees, contractors, and third-party service providers handling RuraRide data.
 - All forms of information processed by the company, whether electronic or physical.
-

3. Security Objectives

RuraRide's primary security objectives are to:

1. Protect user and driver data from unauthorized access.
 2. Maintain confidentiality, integrity, and availability of all systems.
 3. Ensure secure payment processing through verified and compliant partners.
 4. Detect, respond to, and recover from any security incidents effectively.
 5. Foster a culture of continuous security awareness among staff and users.
-

4. Information Security Principles

4.1 Confidentiality

All data processed by RuraRide is treated as confidential. Only authorized personnel have access to sensitive systems and data, strictly on a **role-based access control (RBAC)** model.

4.2 Integrity

We ensure that information remains accurate and complete through encryption, access logging, and real-time monitoring to prevent unauthorized modifications.

4.3 Availability

RuraRide's systems are designed for high availability. Redundant infrastructure, backup systems, and cloud-based resilience ensure minimal downtime for users and drivers.

5. Data Encryption & Storage

- All communication between user devices, servers, and third-party systems is protected using **SSL/TLS encryption**.
- Sensitive data such as passwords, tokens, and identity verification documents are **encrypted at rest** using AES-256 encryption.
- Payment card information is **not stored** on RuraRide's servers; it is securely handled by **PayFast**, our PCI DSS-compliant partner.
- Regular database backups are performed to ensure data recovery capability in the event of failure or corruption.

6. Authentication & Access Control

- All administrative access requires **multi-factor authentication (MFA)**.
- Passwords must meet complexity standards (minimum 8 characters, alphanumeric + symbols).
- User sessions are automatically logged out after a period of inactivity.
- System logs are reviewed periodically to detect unauthorized access attempts.

For drivers and riders, authentication tokens are managed securely and expire regularly to maintain session safety.

7. Application & Network Security

- The RuraRide application undergoes regular **penetration testing** and **vulnerability assessments** to identify and fix potential risks.
 - All code is reviewed and tested in staging environments before deployment.
 - Firewalls and Intrusion Detection Systems (IDS) protect the network infrastructure.
 - DDoS protection and traffic monitoring help maintain service uptime and prevent abuse.
-

8. Payment Security

RuraRide uses **PayFast** to process all online transactions. PayFast maintains full compliance with **PCI DSS**, ensuring that:

- All credit/debit card data is transmitted securely via SSL encryption.
 - Card information is tokenized and never exposed to RuraRide systems.
 - Transactions are monitored in real time for fraud prevention.
 - Payments are processed in **South African Rand (ZAR)** as per compliance requirements.
-

9. Incident Response & Breach Notification

If a data breach or cybersecurity incident occurs:

1. The issue is logged and escalated to the **Chief Information Security Officer (CISO)** or equivalent role.
 2. A full investigation is launched to determine cause, impact, and mitigation.
 3. Affected users and relevant authorities (including the **Information Regulator of South Africa**) are notified in accordance with POPIA within the prescribed timelines.
 4. Preventative measures are strengthened to reduce recurrence risk.
-

10. Physical Security

- Access to RuraRide's physical servers (where applicable) is restricted to authorized personnel only.
- Office access is monitored and controlled through secure entry systems.

- Equipment containing sensitive information is disposed of securely following decommissioning protocols.
-

11. Employee Awareness & Training

All employees undergo **data protection and cybersecurity training** during onboarding and at regular intervals thereafter.

They are required to adhere to internal IT policies and sign confidentiality agreements. Breach of security responsibilities may result in disciplinary action or termination.

12. Third-Party Service Providers

RuraRide partners only with third-party vendors that maintain equivalent or higher security standards.

Before engagement, vendors undergo security due diligence to ensure compliance with POPIA, PCI DSS, and other relevant standards.

13. Continuous Improvement

Security is an ongoing process. RuraRide conducts:


- **Quarterly system audits**
- **Annual security assessments**
- **Routine patch management and software updates**

We continuously adapt our security posture in line with emerging threats and industry best practices.

14. Contact Information

If you suspect a security issue or wish to report a vulnerability, please contact:

 info@ruraride.co.za

 **+27 (0)63 370 8515**

 www.ruraride.co.za