Data Handling Documentation

Released: 26 February 2025 | Classification: Public

1. Overview

This document provides deep insight into the technical and organizational measures Saletick employs to ensure the **Security, Integrity, and Availability** of data handled through our business platform.

2. Data Roles

Saletick operates under two distinct roles depending on the data type:

Data Controller	For the personal information of our merchants (you).
Data Processor	For inventory data, staff lists, and end-customer records that you manage through our app.

3. Data Collection and Storage

We treat your data with the highest sensitivity:

- **Tier-1 Hosting:** Data is hosted in world-class data centers (AWS/DigitalOcean) with 99.9% uptime.
- **Hardened Encryption:** AES-256 encryption for data at rest and TLS 1.3 for all data in transit.
- **Redundancy:** Daily incremental backups ensure that your business records are never lost.

AES-256 At-Rest Encryption	**TLS 1.3 In-Transit**	**99.9% Uptime SLA**	**Daily Backups**

4. Access Control

We maintain a **"Least Privilege"** access model:

- **Internal Security:** Only authorized engineering staff with Multi-Factor Authentication (MFA) can access production systems.
- **Merchant Security:** Your data is isolated — no other merchant can view your records. You control staff roles and permissions within your business.

5. Data Lifecycle Management

We manage data from creation to destruction:

Input	Minimal data required for core business functionality.

Active Phase	Continuous monitoring and vulnerability scanning.
Deletion	Upon account closure, all active business data is purged within 30 days. Archive backups follow a secondary 60-day turnover policy.

6. Sub-processors

We rely on qualified service providers to deliver parts of our platform (e.g., Paystack for payments, SendGrid for notifications).

> **Note:** All sub-processors undergo a security vendor assessment and are required to provide the same level of protection documented here.

7. Technical Security Measures

Our defense-in-depth strategy includes:

- **WAF (Web Application Firewall)** to block malicious traffic.
- **DDoS protection** layers.
- **Argon2 hashing** for password security.
- **Automated security patching** of all server environments.

8. Audit and Compliance

We don't just set policies — we verify them. Saletick conducts recurring internal audits and works with third-party security firms to simulate attacks (penetration testing) and identify potential weaknesses before they can be exploited.

9. Contact

For technical questions regarding our security architecture or data handling procedures:

Security Team	security@saletick.net
Data Protection Officer (DPO)	privacy@saletick.net