# Smartix Incident Response Policy

Last Updated: 11th December 2025

## 1. Introduction

This Incident Response Policy (“Policy”) describes how Smartix Ltd (“Smartix”, “we”, “our”, “us”) identifies, manages, escalates, and resolves security incidents and personal data breaches.
This Policy is designed to meet the requirements of the UK GDPR, the Data Protection Act 2018, and industry best practices.

Smartix acts as:

- **Data Controller** for Personal Data we collect directly (e.g., customer name, address, phone, email, Stripe references).
- **Data Processor** for encrypted Pass Data transmitted by customers (“Controllers”) for the purpose of generating and managing wallet passes.

Because Pass Data is stored as strongly encrypted records that Smartix does not inspect, Smartix may not be able to determine whether any individual encrypted record contains personal data. This Policy reflects that constraint.

## 2. Definitions

**Security Incident:**
Any event that may compromise the confidentiality, integrity, or availability of systems, data, or services.

**Personal Data Breach:**
A breach of security leading to accidental or unlawful destruction, loss, access, disclosure, or alteration of Personal Data. For encrypted Pass Data, Smartix treats any unauthorised access as a potential personal data breach because we cannot determine whether a compromised record contained personal data.

**Operational Incident:**
A non-security event that impacts service functionality (e.g., outages, performance degradation).

# Smartix Incident Response Policy

## 3. Incident Detection

Smartix detects incidents through:

- AWS CloudWatch logs and Lambda execution logs
- Application-level error reporting
- RDS error and performance logs
- AWS service health notifications
- System anomalies observed during routine operational monitoring
- Customer-reported issues or suspicious activity notifications
- Subprocessor notifications (AWS, Stripe, Apple, Google)

Smartix may add or evolve monitoring mechanisms over time as the platform grows.

# Smartix Incident Response Policy

## 4. Severity Classification

Smartix assigns each incident a severity level to determine the response actions.

### 4.1. Critical Severity

Events including:

- Unauthorised access to systems containing Controller data (including encrypted Pass Data)
- Unauthorised access to Smartix-controlled Personal Data
- Compromise, suspected compromise, or misuse of encryption keys or access paths to encrypted data
- System-wide outage affecting all customers
- Any event where Smartix cannot rule out a risk to personal data

### 4.2. High Severity

Events including:

- Attempted intrusion or compromise
- Outage affecting multiple customers
- Misconfigurations that could expose data if unaddressed
- Degradation of critical systems (e.g., persistent Lambda failures, RDS issues)
- Failures of key dependencies (e.g., KMS availability problems)

### 4.3. Low Severity

Events including:

- Routine operational anomalies
- Transient or minor outages
- Lambda execution errors without data risk
- API throttling
- CloudWatch warnings
- Issues affecting only a small subset of customers
- Problems that can be corrected without impacting confidentiality or integrity of data

# Smartix Incident Response Policy

## 5. Incident Response Workflow

All incidents follow these phases:

### 5.1. Identification

Smartix evaluates incoming alerts, logs, customer reports, or system anomalies to confirm whether an incident has occurred.

### 5.2. Containment

Immediate actions may include:

- Isolating affected components
- Revoking credentials or API keys
- Disabling affected services
- Blocking suspicious traffic
- Rotating KMS keys (if applicable)

### 5.3. Assessment

Smartix assesses:

- Severity level
- Systems and data affected
- Whether encryption keys or encrypted data were involved
- Whether Smartix-controlled Personal Data was accessed
- Whether Pass Data **may** have been exposed (even if not readable)

Because Smartix cannot inspect encrypted Pass Data, any unauthorised access to encrypted records is treated as a potential personal data incident for notification purposes.

### 5.4. Eradication & Fix

Smartix resolves root causes by:

- Patching or reconfiguring systems
- Removing malicious code or access
- Restoring from clean states
- Re-deploying infrastructure components

# Smartix Incident Response Policy

## 5.5. Recovery

Smartix restores normal service operation and monitors affected systems for recurrence.

## 5.6. Notification

Notifications depend on data roles:

### 5.6.1. If Smartix is Processor (Pass Data)

Smartix notifies the Controller *without undue delay* of any incident involving access to, or potential risk to, encrypted Pass Data.
Smartix does **not** notify the ICO; that is the Controller's responsibility.

### 5.6.2. If Smartix is Controller (account data)

Smartix assesses whether notification to the ICO or affected individuals is required under UK GDPR (within 72 hours).

## 5.7. Post-Incident Review

Smartix conducts internal reviews to document:

- timeline of events
- lessons learned
- improvements to processes or systems
- prevention measures for future incidents

# Smartix Incident Response Policy

## 6. Roles and Responsibilities

### 6.1. Incident Manager

- Oversees the incident response
- Coordinates communication
- Ensures documentation of actions taken

### 6.2. Engineering Lead

- Investigates technical causes
- Implements containment and fixes
- Reviews logs and system-level evidence

### 6.3. Security Contact / Data Protection Lead

- Assesses GDPR implications
- Coordinates breach notifications to Controllers
- Advises on evidence preservation
- Supports the post-incident review

### 6.4. Support Team

- Communicates updates to affected customers (as instructed)
- Collects relevant information from customer reports

For smaller-scale incidents, one person may fulfil multiple roles.

# Smartix Incident Response Policy

# 7. Communication and Notification

## 7.1. Notification to Controllers

For incidents involving Pass Data, Smartix will notify the Controller:

- without undue delay
- with available information, including:
    - nature of the incident
    - systems or encrypted data potentially affected
    - containment and mitigation measures taken
    - recommended next steps

## 7.2. Notification to ICO or Data Subjects

Smartix notifies the ICO **only** where Smartix-controlled Personal Data is affected, and only when legally required.

Smartix does **not** notify data subjects for Pass Data; this responsibility lies with the Controller.

## 7.3. Communication to Subprocessors

Smartix monitors and acts upon notifications from AWS, Stripe, Apple, and Google where relevant.

# 8. Logging and Evidence Preservation

Smartix preserves relevant logs and evidence during an incident, including:

- CloudWatch logs
- Lambda execution traces
- RDS logs
- Authentication and access records
- Deployment records

Logs may contain metadata but not decrypted Pass Data.

# Smartix Incident Response Policy

## 9. Testing and Review

Smartix reviews this Policy annually and:

- tests elements of the incident workflow when feasible
- updates procedures as the platform evolves
- incorporates security improvements from lessons learned

## 10 Download PDF

## 11. Contact Information

If you have questions about this Policy or wish to report a security concern, please contact us at:

www.smartix.uk/contact