uncletimdigital@gmail.com | 08107198344
UNCLETIMTECH.COM

RISK ASSESSMENT AND INCIDENT RESPONSE PLAN

Version 1.0 | Effective: 2 November 2026 | Owner: Director / DPO | Review: Annually or after any major change

1. Risk assessment approach

UNCLETIM identifies, scores, and treats information and operational risks at least annually and whenever a significant change occurs. Each risk is scored for likelihood (1–5) and impact (1–5); the product gives the rating. Risks rated high (15+) require treatment plans with owners and dates; all risks are recorded in a risk register reviewed quarterly by the Director.

2. Principal risks and treatments (summary register)

Risk	Rating	Key treatments
Fraudulent wallet transactions / social engineering	High	Transaction monitoring, customer verification via Prembly, 9PSB fraud-alert duties (acknowledge 1 hour, lien 30 minutes, resolve 72 hours), staff awareness training
Compromise of API keys or credentials	High	MFA on all access, secrets held in a credential vault, API key rotation every 90 days, least-privilege access, immediate revocation procedure
Personal data breach	High	Encryption in transit (TLS 1.2+) and at rest (AES-256), access controls, NDPA breach procedure — notify NDPC within 72 hours where required
Partner outage (9PSB / Prembly)	Medium	Business Continuity Plan, customer communication templates, reconciliation on restoration
Insider misuse of access	Medium	Unique user IDs, no shared accounts, quarterly access reviews, audit logs retained for two (2) years
Malware / ransomware	Medium	Endpoint protection, patching, daily cloud backups, staff phishing awareness

3. Incident classification

- P1 – Critical: active fraud, confirmed data breach, or full service outage. Response begins immediately.
- P2 – High: attempted intrusion, suspected credential compromise, partial outage. Response within 2 hours.
- P3 – Medium: malware on a single device, policy violation. Response within 1 business day.
- P4 – Low: minor events and near-misses. Logged and reviewed monthly.

4. Incident response procedure

- Detect and report: any staff member reports a suspected incident to the Director immediately by phone.
- Assess and classify: the Director classifies the incident, opens an incident record, and assembles the response (Director, plus external specialists where needed).
- Contain: isolate affected systems/accounts, revoke compromised credentials and API keys, and — for fraud — comply with 9PSB timelines (acknowledge alerts within 1 hour, effect liens within 30 minutes, resolve within 72 hours).
- Notify: notify 9PSB and other affected partners without undue delay; where a personal data breach is likely to risk individuals' rights, notify the Nigeria Data Protection Commission within 72 hours as required by section 40 of the Nigeria Data Protection Act 2023, and inform affected data subjects where required.
- Eradicate and recover: remove the root cause, restore from clean backups, and verify integrity before returning to service.
- Lessons learned: document the incident, timeline, and corrective actions in the incident register; update this plan and the risk register accordingly.

5. Review

This plan is reviewed annually, after every P1/P2 incident, and after any major system or partner change.

Approved and signed:



Olamide Timilehin Adedayo
Director, Uncletim Digital Solutions LTD
Date: 2 November 2026