APHELION · TRUST CENTER

Security Whitepaper

How Aphelion secures, operates and recovers the cloud, AI and managed services that power enterprises across Africa, Europe and the Indian Ocean.

Document	Security Whitepaper
Version	v1.0 · 05 August 2026
Classification	Public
Owner	Data Protection Officer, Aphelion Ltd.
Contact	dpo@aphelion-group.com · +230 248 3744

This document is published under the Aphelion Trust Center and is available for download at aphelion-group.com/trust-center.

SECTION 01

Executive Summary

Aphelion Ltd. is the leading Cloud, AI and Managed Services provider in Mauritius, serving 80+ enterprises across 11 countries. For over 17 years we have run mission-critical systems for banks, insurers, BPOs, ISPs, retailers, hotel groups, healthcare providers, telecom operators, universities and real-estate developers.

This whitepaper documents the security, compliance and operational posture that underpins every engagement. It is intended for procurement, security, risk and compliance teams evaluating Aphelion as a managed services partner. The controls described here apply to every managed workload by default; sector-specific extensions (HIPAA, SOC 2, IEC 62443) are applied per client and documented in the service agreement.

Posture at a glance

Compliance	ISO 27001, ISO 9001, ISO 20000, GDPR, Mauritius DPA 2017, PCI-DSS
Uptime SLA	99.99% on managed infrastructure (99.999% on carrier-grade engagements)
Incident response	<15 minutes mean P1 response, 24/7, every day of the year
Ransomware recovery	RPO <4 hours · RTO <4 hours · tested quarterly
SOC model	24/7 Broadsword MDR with named analysts and tested breach-response playbooks
Data residency	On-island default (Riche Terre, Mauritius); partner facilities across the Indian Ocean and Africa
Encryption	TLS 1.2+ in transit, AES-256 at rest, customer-managed keys on request
Personnel	Background-checked engineers, MFA on all access, annual security training

SCOPE

This whitepaper covers managed cloud, cybersecurity (Broadsword MDR), backup & disaster recovery, network & connectivity, AI (Tailwind Labs) and digital workplace services. Software development and advisory engagements follow the same security baselines for source code, repositories and deliverables.

SECTION 02

Compliance & Certifications

Aphelion operates to a multi-framework compliance posture. Every engagement inherits the controls below; sector-specific frameworks are layered on top per client requirement and documented in the service agreement.

Framework	Scope	Status
ISO 27001	Information security management — people, process, technology	Compliant
ISO 9001	Quality management — service delivery, change, continuous improvement	Compliant
ISO 20000	IT service management — ITIL processes for incident, problem, change	Compliant
GDPR	Lawful processing, data subject rights, international transfers	Compliant
Mauritius DPA 2017	National data protection — controller/processor obligations	Compliant
PCI-DSS	Cardholder data — tokenisation, segmentation, audit trails	Compliant

Sector-specific extensions

- HIPAA — applied for healthcare and international patient-data workloads.
- SOC 2 — Type II reports available under NDA for due-diligence reviews.
- IEC 62443 — OT/IT converged infrastructure for manufacturing and logistics.
- ICT Authority Mauritius — telecom operator requirements for carrier-grade engagements.

AUDIT & ASSURANCE

Compliance evidence is available to clients under NDA via the Aphelion Trust Center. Annual independent audits, penetration test summaries and the latest ISO certificates are provided during the procurement and onboarding phases.

SECTION 03

Data Residency & Sovereignty

Data residency is the foundation of trust for our clients. By default, managed workloads run in our Riche Terre, Mauritius data centre with documented data flows and right-to-erasure controls aligned to the Mauritius Data Protection Act 2017 and the EU GDPR.

Residency tiers

- **On-island (default)** — workloads and primary data stay in Mauritius. Suitable for regulated industries and clients with strict residency requirements.
- **Regional** — workloads may run in partner facilities across the Indian Ocean and Africa, with documented cross-border transfer mechanisms (SCCs, adequacy).
- **Public cloud regions** — workloads may run in client-selected public cloud regions (Azure, AWS), with residency documented per workload.
- **Sovereign cloud** — air-gapped or sovereign-cloud deployments for national-security-grade workloads, with full cryptographic sovereignty.

Data flow documentation

Every engagement produces a documented data flow map showing where each data class physically resides, who can access it, and which subprocessors are involved. Right-to-erasure requests are honoured under the documented SLA in the service agreement, with regulator-ready reporting available on demand.

CROSS-BORDER TRANSFERS

Where data leaves Mauritius or the European Economic Area, we rely on applicable safeguards including adequacy decisions, Standard Contractual Clauses or other lawful transfer mechanisms, and we document the transfer in our records.

SECTION 04

Encryption

Encryption is applied by default across every layer of the stack. Customer-managed keys are available for workloads that require cryptographic sovereignty.

Layer	Standard	Notes
In transit	TLS 1.2+ (TLS 1.3 preferred)	Mandatory on all external and internal APIs; HSTS enforced
At rest	AES-256	Default for all storage classes (block, object, database)
Key management	KMS / HSM-backed	Per-tenant keys with rotation policies
Customer-managed keys	BYOK / HYOK	Available for sovereign workloads; client holds key material
Backups	AES-256 + immutable	Air-gapped copies; encryption keys separated from backup storage
Email & messaging	TLS + opportunistic DANE	Inbound and outbound; M365 Message Encryption for sensitive content

Cryptographic lifecycle

- Certificates are issued via a managed PKI; automated renewal with 30-day expiry alerts.
- Symmetric keys are rotated annually or on personnel change, whichever is sooner.
- Decommissioned storage media is cryptographically erased or physically destroyed with a certificate of destruction.
- Cryptographic standards are reviewed annually against the latest NIST and ENISA guidance.

SECTION 05

Access Control

Access to client environments follows a zero-trust model: identity-first, least-privilege, micro-segmented. No standing production access is granted to any individual by default — elevation is just-in-time and audit-logged.

Identity & authentication

- Phishing-resistant MFA (FIDO2 / WebAuthn) on every privileged account.
- Centralised identity provider (Microsoft Entra ID) with conditional access policies.
- Separation of duties between development, operations and security teams.
- Service accounts use workload identity federation where supported; long-lived credentials are prohibited.

Authorisation

- Role-based access control (RBAC) with documented role definitions per client environment.
- Just-in-time elevation via a break-glass workflow with named approvers and time-boxed grants.
- Quarterly access reviews — every active grant is re-confirmed by the client and an Aphelion engineering lead.
- Network segmentation between client environments, management planes, and PCI/HIPAA-scoped zones.

AUDIT TRAIL

Every authentication, authorisation change, and privileged action is logged to an append-only SIEM with a 12-month hot retention and 7-year cold retention. Logs are available to clients for forensic review under the service agreement.

SECTION 06

Monitoring & Incident Response

Monitoring and incident response are operated 24/7 by the Broadsword Security Operations Centre. Broadsword is Aphelion's AI-driven Managed Detection & Response (MDR) platform — it correlates endpoint, identity, cloud and network telemetry, with human triage on every P1 alert.

Detection coverage

- Endpoint Detection & Response (EDR) on every managed endpoint.
- Cloud workload protection for IaaS and PaaS services.
- Identity anomaly detection (impossible travel, MFA fatigue, token theft).
- Network traffic analysis and north-south / east-west flow monitoring.
- Deception technology (honeytokens, canary files, fake endpoints) for early breach detection.

Incident response process

Step	Phase	Target	Description
1	Detect	Continuous	SIEM correlation surfaces candidate incidents within minutes.
2	Triage	<15 min (P1)	Named SOC analyst confirms severity; client contact notified.
3	Contain	Minutes	Automated playbooks isolate hosts, revoke credentials, block indicators.
4	Eradicate & recover	Hours	Root cause removed; systems rebuilt from known-good images; backups validated.
5	Review & harden	10 business days	Written post-incident report with timeline, root cause and hardening actions.

BREACH NOTIFICATION

Clients are notified of confirmed security incidents affecting their environment without undue delay and within the timelines defined in the service agreement and applicable regulation (GDPR Article 33: 72 hours where applicable).

SECTION 07

Business Continuity & Disaster Recovery

Business continuity is engineered into every managed environment. Recovery objectives are agreed per workload in the service agreement and tested quarterly via DR drills.

Objective	Target	How we meet it
Recovery Point Objective (RPO)	<4 hours	Continuous replication + immutable snapshots
Recovery Time Objective (RTO)	<4 hours	Tested recovery runbooks + standby capacity
Uptime SLA (managed infra)	99.99%	Redundant power, cooling, carrier diversity, automated failover
Uptime SLA (carrier-grade)	99.999%	2N power, diverse routes, multi-az deployment
Backup testing	Quarterly	Full restore drills with documented results
Ransomware drill	Quarterly	End-to-end tabletop + live recovery from immutable backups

Backup architecture

- 3-2-1 strategy: three copies of data, on two media types, with one off-site.
- Immutable, air-gapped backup copies that cannot be modified or deleted by ransomware.
- Geo-replication to a secondary facility for regional disaster scenarios.
- Backup integrity validation on every backup job — silent corruption is detected and alerted.

Business continuity planning

Each client engagement includes a documented Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP). Plans are reviewed annually and after any material change to the environment. Crisis communication protocols, escalation paths and client-side contacts are maintained in a living document.

SECTION 08

Personnel Security

Our people are the front line of our security posture. Every engineer and analyst is background-checked, trained and accountable to a named client engagement.

Pre-employment

- Background checks including criminal record, employment history and qualification verification.
- NDAs and confidentiality agreements signed before any access to client systems.
- Role-specific security induction completed within the first 30 days of employment.

During employment

- Annual mandatory security awareness training, including phishing simulations.
- Role-based training: SOC analysts complete SANS/GIAC paths; cloud engineers complete vendor certifications.
- Acceptable Use Policy governs device, network and information handling.
- Clean-desk and clear-screen policies enforced in operational areas.

Off-boarding

- Access revoked within 1 hour of termination notice.
- Exit interview includes confirmation of returned assets and reaffirmation of confidentiality obligations.
- Client environments are notified of personnel changes affecting their named engineers.

NAMED-ENGINEER MODEL

Unlike faceless helpdesks, Aphelion assigns named engineers accountable for each client environment. This creates direct accountability, faster escalation, and a single point of contact who knows your stack — and who is on call when something breaks at 3am.

SECTION 09

Vulnerability Management

Vulnerability management is a continuous, defence-in-depth practice — not a once-a-year checkbox. We operate scanning, patching, testing and red-teaming across every layer of the stack.

Activity	Frequency	Scope
Continuous vulnerability scanning	Daily	All managed hosts, containers and cloud services
Authenticated operating-system patching	Monthly	Critical patches within 7 days; high within 30 days
Application dependency scanning (SCA)	On commit + weekly	Open-source libraries in client and internal codebases
Static & dynamic application testing (SAST/DAST)	Per release	Web and mobile applications we build or operate
External penetration testing	Annually	Independent third-party; report within 10 business days
Internal red-team exercise	Annually	Full kill-chain simulation against Broadsword defences

Disclosure & remediation

- Vulnerabilities are scored using CVSS v3.1 and triaged into severity-based SLAs.
- Critical (CVSS 9.0+) — patched or mitigated within 7 days.
- High (CVSS 7.0–8.9) — patched within 30 days.
- Medium / Low — scheduled into the next change window.
- Clients receive a vulnerability summary in their quarterly service review.

COORDINATED DISCLOSURE

Aphelion accepts responsible disclosure reports from external researchers at security@aphelion-group.com. We commit to acknowledgement within 1 business day and to coordinated publication of fixes and advisories.

SECTION 10

Contact & Document Control

Questions about this whitepaper, security due-diligence requests and breach notifications should be directed to the contacts below. We respond within one business day.

Role	Contact	Purpose
Data Protection Officer (DPO)	dpo@aphelion-group.com	GDPR / DPA queries, data subject rights, residency
Security Operations Centre	soc@aphelion-group.com · +230 248 3703	24/7 incident reporting, MDR escalation
Trust & Assurance	trust@aphelion-group.com	Audit evidence, whitepaper questions, due diligence
Responsible disclosure	security@aphelion-group.com	External researcher vulnerability reports
General enquiries	info@aphelion-group.com · +230 248 3744	Pre-sales, onboarding, account management

Document control

Document title	Aphelion Security Whitepaper
Version	v1.0
Publication date	05 August 2026
Classification	Public
Owner	Data Protection Officer, Aphelion Ltd.
Review cycle	Annual or on material change
Next review	12 months from publication date
Distribution	Public — available at aphelion-group.com/trust-center
Format	PDF, A4, dark cosmic print theme

Change log

Version	Date	Summary
1.0	05 August 2026	Initial publication. Covers sections 01–10 as listed in the contents.