AI UNITI
Information Security Policy

v2.0
Effective 23 May 2026
AI Uniti Pty Ltd | ACN 694 238 821

Information Security Policy

AI Uniti's commitments and controls for protecting information assets

Document	Information Security Policy
Version	v2.0 (Final)
Effective date	23 May 2026
Supersedes	v1.x (general statements only)
Owner	Andrew Scully, COO (security accountable executive)
SOC 2 Type I target	Q4 FY26 (auditor engagement signed; evidence collection in Vanta)

1. Scope and applicability

This Information Security Policy describes the technical and organisational measures that AI Uniti Pty Ltd (ACN 694 238 821) implements to protect information assets, including Customer Data and Personal Data processed in connection with its products. It applies to all AI Uniti products (Pulse Check, Signal, Unite), all AI Uniti environments (production, non-production, corporate), and all AI Uniti personnel (employees, contractors, and authorised vendors).

2. Information security objectives

AI Uniti's information security program is designed to achieve:

- confidentiality of Customer Data and Personal Data;
- integrity of data and systems supporting the Services;
- availability of the Services in accordance with the applicable service commitments;
- compliance with the Privacy Act 1988 (Cth), the GDPR (where applicable), and the data protection commitments in the DPA;
- alignment with the AICPA Trust Services Criteria, as evidenced by the SOC 2 Type I engagement under way (see section 4).

3. Governance and ownership

The COO is the security-accountable executive and chairs the AI Uniti Security Forum. The CTO holds technical accountability for production environments and engineering controls. Security policies are reviewed at least annually, on material architectural change, and following any significant incident.

4. Security framework and certifications

AI Uniti is pursuing SOC 2 Type I certification, with completion targeted for Q4 FY26. The auditor engagement is signed; evidence collection is automated through Vanta as the compliance evidence platform. Following Type I, AI Uniti intends to progress to SOC 2 Type II within the following audit period.

AI Uniti's control framework is mapped to the AICPA Trust Services Criteria (Security, Availability, Confidentiality) and aligned with ISO 27001 control families. AI Uniti will share the SOC 2 report and bridge letters with customers under NDA on request, once issued.

5. Access control

- Role-based access control (RBAC) with least-privilege defaults. New access is provisioned only by approved request; standing administrative access is minimised.
- Multi-factor authentication (MFA) is required for all administrative access to production environments and corporate identity systems.
- Single sign-on (SSO) via the customer's identity provider is supported for enterprise customers (SAML 2.0, OIDC).
- Quarterly access reviews. Joiner-mover-leaver controls trigger access change within one business day; production access is revoked on employment end within four hours.
- Privileged access uses just-in-time elevation with audit logging.

6. Encryption

- Data in transit is protected with TLS 1.2 or higher for all external connections; internal service-to-service traffic uses mutual TLS where supported.
- Data at rest is encrypted with AES-256 or an equivalent symmetric algorithm using managed key services (AWS KMS in the default deployment).
- Customer-managed keys are available for Enterprise customers on the default cloud deployment, subject to the Order Form.
- Cryptographic keys are rotated on schedule (at least annually) and on personnel change for key custodians.

7. Network security

- Production environments are segregated from corporate and non-production environments.
- Default-deny ingress at the perimeter. Egress controls are applied to production workloads.
- Web application firewall and DDoS protection at the edge (Cloudflare).
- VPC segmentation, private subnets for data tier, no public exposure of databases or model-serving endpoints.
- Customer environments in the multi-tenant SaaS are logically segregated; tenant boundary enforcement is tested in CI for the shared intelligence layer.

8. Endpoint and personnel device security

- All personnel devices used to access production or Customer Data are managed (disk encryption enforced, screen lock enforced, OS up to date, EDR installed).

- Personal devices are not permitted for production access.
- Removable media is restricted and audited.

9. Vulnerability and patch management

- Dependency scanning runs on every commit; critical vulnerabilities block deployment.
- Container and image scanning runs on build; base images are rebuilt at least monthly.
- External penetration testing is conducted at least annually once the SOC 2 program is under way, by an independent provider; remediation tracked to closure.
- Critical vulnerabilities are patched within 7 days of public disclosure; high within 30 days; medium within 90 days.

10. Logging, monitoring, and detection

- Security-relevant events (authentication, authorisation, configuration change, data access on sensitive paths) are logged centrally.
- Logs are retained for a minimum of 12 months, write-once where the platform supports it.
- Anomaly detection is in place for authentication events, privileged access, and key data flows.
- On-call security response is available 24x7.

11. Incident response and breach notification

AI Uniti maintains a documented incident response plan that defines roles, severity classification, escalation paths, communication protocols, and post-incident review. Tabletop exercises are conducted at least annually.

In the event of a Personal Data Breach affecting Customer Personal Data, AI Uniti notifies the affected customer without undue delay and in any event within 72 hours of becoming aware, in accordance with section 12 of the DPA. AI Uniti cooperates with customers and regulators in any subsequent investigation.

12. Business continuity and disaster recovery

- Production data is backed up on a defined schedule (full daily, incremental hourly for primary stores) with backup integrity tested quarterly.
- Recovery Point Objective (RPO): 1 hour for primary data stores.
- Recovery Time Objective (RTO): 4 hours for the Services.
- Disaster recovery procedures are documented and exercised at least annually.

13. Personnel security

- Background checks (including verification of identity, work eligibility, and adverse-record checks where lawfully permitted) for all personnel with production access.
- Security awareness training on hire and annually thereafter, with role-specific training for engineering personnel.
- Written confidentiality, acceptable-use, and intellectual property assignment agreements for all personnel.

- Documented and enforced offboarding procedure with access revocation on the day of departure.

14. Sub-processor security

AI Uniti conducts security due diligence on each Sub-processor before engagement, reviewing certifications, data protection commitments, and incident history. Every Sub-processor is contractually bound to security obligations no less protective than this Policy and the DPA. Sub-processor posture is reviewed at least annually and on material change.

15. Customer-controlled deployments

Where a customer elects an alternative region, alternative cloud provider, or on-premises deployment under section 2 of the Subprocessor Disclosure, the allocation of security responsibility shifts accordingly.

- For alternative cloud regions and providers: AI Uniti remains responsible for application-layer and shared-platform controls; the cloud provider's underlying controls apply at the infrastructure layer.
- For on-premises deployments: AI Uniti remains responsible for application-layer controls (authentication, authorisation, audit logging, encryption configuration); the customer is responsible for infrastructure security (host hardening, network controls, backup, monitoring). AI Uniti provides reference hardening guidance and configuration baselines.

16. Audit and assurance

AI Uniti will make available to customers, on reasonable request and under NDA:

- the current SOC 2 report (once issued) and bridge letters between audit periods;
- summary results of the most recent external penetration test;
- this Information Security Policy and the Subprocessor Disclosure;
- responses to standard security questionnaires (CAIQ, SIG Lite, or equivalent).

Direct customer audits are available in accordance with section 15 of the DPA.

17. Review and updates

This Information Security Policy is reviewed at least annually and on material architectural change. Material changes are notified to customers as part of the change-notification process under the DPA.

18. Contact

Security enquiries and incident reports: security@aiuniti.com. PGP key fingerprint available on request.

End of Information Security Policy v2.0. Effective 23 May 2026.