VENDOR SECURITY & PRIVACY

Security Information Pack

Information security, privacy, data protection and cyber control overview

Prepared for	Council procurement, ICT and security teams
Prepared by	PlanSuite Pty Ltd | ABN 57 691 312 795
Version	1.0 | Issued 30 July 2026
Status	External, issued for council procurement and security review
Document owner	Director, PlanSuite Pty Ltd

Executive summary

PlanSuite is a web-based, AI-assisted statutory planning platform built for Victorian planning workflows. It provides mapping, planning advice, chat, document analysis and report generation for councils and planning professionals.

Our security position centres on Australian-hosted production infrastructure, encryption in transit and at rest, organisation-based access controls, restricted administration, monitored cloud services, managed backups, transparent subprocessor disclosure and human review of AI-assisted outputs.

> **Procurement position**
>
> This pack does not claim ISO 27001, SOC 2, IRAP, independent Essential Eight certification or an independent penetration-testing report. Our platform is aligned with the ASD Essential Eight, as set out in section 10. Where an assurance artefact is not held, we say so rather than imply certification.

Security at a glance

Domain	PlanSuite position	What it means for council
Hosting	AWS Sydney (ap-southeast-2)	Customer data is stored in Australia.
Encryption	HTTPS/TLS in transit; AWS-managed encryption at rest	Uploaded plans and documents are encrypted in storage and in transit.
Access	Authenticated accounts, RBAC, restricted internal administration	Council users only see data within their own organisation.
SSO & MFA	Optional SSO with the council's identity provider; council IdP controls MFA	Supports Microsoft Entra ID, Okta and other SAML/OIDC providers.
Backups	Managed database backups with point-in-time recovery; document storage versioning	Backups are encrypted with a dedicated key and held in the Sydney region.

Domain	PlanSuite position	What it means for council
AI use	Google Vertex AI via API; customer data is not used to train models	Planner review remains required before reliance on any output.
Incident notification	Affected customers notified within 72 hours of confirming a breach affecting customer data	Contractual commitment; statutory notification obligations apply separately.
Data ownership	The customer retains ownership of uploaded data	We do not sell personal data.
Essential Eight	Aligned across seven strategies; Office macros not applicable	Self-assessed alignment; no independent maturity-level assessment is claimed.

1. Service & security context

PlanSuite is delivered as Software as a Service through a web browser. The Council Starter Package is designed to operate alongside existing council systems without local installation or mandatory document-management integration. Council users save generated Word outputs into existing records systems through their normal processes.

- No PlanSuite software is installed on council endpoints or networks.
- Council access can be configured with optional SSO using the council's identity provider.
- Council users, modules, local planning resources and optional integrations are configured during onboarding.
- Uploaded plans and documents are used by PlanSuite report workflows and are never publicly accessible.
- AI-assisted outputs are preliminary and remain subject to planner verification and decision-making.

High-level architecture

Component	Security / data role
Council user	Web browser access over HTTPS/TLS.
PlanSuite application	Containerised web application on AWS ECS Fargate.
Data services	Managed AWS RDS database and AWS S3 document storage, with encryption at rest, automated backups and object versioning.
Planning data	Official Victorian Government sources including VicPlan, Vicmap and Victorian GeoServer.
AI processing	Google Vertex AI accessed through API. Customer data is not used to train the underlying models.
Supporting services	Mapping, transactional email, in-product support, billing and error monitoring, as disclosed in section 7.

2. Data handling & information lifecycle

Information categories

- Account information, including the user and organisation details required to provide access.
- Uploaded planning documents, plans and related materials supplied by users.
- Property and planning information obtained from official data sources.
- Usage and technical information used to operate and secure the service.
- Generated reports, letters and planning analysis produced through PlanSuite workflows.

Lifecycle controls

Stage	Control
Collect	Collect only the information needed for accounts, service delivery, document analysis, support and security.
Transmit	Protect user-to-platform traffic using HTTPS/TLS.

Stage	Control
Process	Process information within PlanSuite and the disclosed service providers required for the requested functionality.
Store	Store customer data in AWS Sydney (ap-southeast-2) using managed cloud services.
Access	Restrict access using authenticated accounts, RBAC, organisation boundaries and restricted internal administration.
Retain	Retain information only as long as reasonably required for operational or legal purposes.
Delete	Users may delete properties and uploaded content from the platform at any time. Full account or organisation data deletion is actioned on request. After termination, a customer may request export of its data in a standard format within 30 days, after which data may be deleted unless retention is required by law.

3. Infrastructure, encryption & platform security

Cloud infrastructure

PlanSuite is hosted on Amazon Web Services in the Sydney region (ap-southeast-2), using AWS ECS Fargate for the application runtime, AWS RDS for managed database infrastructure and AWS S3 for document storage.

- ECS Fargate provides a managed container runtime. Only our verified, containerised application code executes in production.
- AWS manages the underlying Fargate host operating system and host-level patching.
- AWS RDS provides managed database infrastructure with automated backups and point-in-time recovery.
- AWS S3 document storage has object versioning enabled in production, and public access is blocked at the bucket level so an object cannot be made publicly readable by misconfiguration.
- Production infrastructure is subject to continuous system monitoring.

Encryption

IMPLEMENTED	**In transit**: data transmitted between users and our servers is encrypted using HTTPS/TLS.
IMPLEMENTED	**At rest**: the production database is encrypted using AWS KMS. Document storage is encrypted with AES-256 server-side encryption applied by default to every object.

Secure application practices

- Automated deployments and version control.
- Regular automated software testing as part of the development lifecycle.
- Automated vulnerability scanning of application dependencies, which raises patch pull requests when a known vulnerability is published.
- Continuous deployment, so security fixes reach production quickly rather than waiting on a release window.
- No Flash, Java applets, web advertising, Office macros, ActiveX controls or PlanSuite executable installation is involved in ordinary platform use.

4. Identity, access & administrative security

- Authenticated user accounts are required for all protected platform information.
- Role-Based Access Control (RBAC) governs application permissions.
- Council users are restricted to data within their own organisation.
- Internal administrative access is restricted and designed around least privilege.
- AWS IAM policies restrict infrastructure access to the required permissions.
- Internal infrastructure access uses short-lived, role-based credentials issued through an identity provider that enforces MFA. The production account holds no long-lived IAM users and no root access keys.
- Centralised root access management is enabled across our AWS organisation. The production account holds no root user credentials and root password recovery is blocked, so there is no root sign-in path to production.
- Access keys and credentials are held in managed secret storage and are never committed to source code or customer outputs.

- Optional SSO connects PlanSuite to the council's existing identity provider, so the council controls staff authentication and MFA policy.
- SSO supports prompt deprovisioning when access is removed at the council identity provider.

> **Shared responsibility**
>
> Where SSO is used, PlanSuite secures the SaaS platform while the council controls identity-provider configuration, MFA policy, user lifecycle, endpoint and browser security, and internal handling of downloaded or generated records.

5. AI security, transparency & human oversight

PlanSuite uses AI to analyse planning information and generate structured outputs. Relevant property data, planning scheme content and user inputs are sent to the AI service via API for processing.

No AI training on council data: council and customer content is used to support the requested service, not to train public AI models.

Where data is stored: all customer data is stored in Australia (AWS Sydney, ap-southeast-2). No customer data is persistently stored offshore.

AI processing & data residency: AI processing is performed via Google Vertex AI. Request content sent for AI processing may be handled outside Australia on a transient basis. Under our terms with Google, this content is not used to train models. Councils with specific data-processing residency requirements should contact PlanSuite to discuss available configuration options.

Enterprise API access: AI services are accessed through an enterprise API, not public consumer accounts.

Output limitations: outputs may be probabilistic, depend on input quality and may contain inaccuracies.

Planner verification: AI-assisted outputs are preliminary guidance. They must be independently reviewed by a suitably qualified planner and must not be the sole basis for a legal, regulatory or statutory decision.

Authoritative sources: assessments read from official Victorian Government data and current planning scheme ordinances, with clause citations so outputs can be verified at a glance.

> **Operational principle**
>
> AI-assisted outputs support professional judgement. Council officers remain responsible for review and decisions.

6. Privacy, data residency & data ownership

- Customer data is stored on AWS infrastructure in Sydney, Australia. Certain disclosed service providers process limited information in other jurisdictions for the applicable service function, as set out in section 7.
- Users retain ownership and control of uploaded data.
- Uploaded documents are never made publicly available and are accessible only to authorised users within the same organisation.
- We do not sell personal data.
- We minimise collection of personally identifiable information wherever possible.
- Personnel with access to customer data are subject to confidentiality obligations under our Data Processing Agreement.
- Our Privacy Policy is governed by the Privacy Act 1988 (Cth) and the Australian Privacy Principles.
- Our security practices are informed by the Privacy and Data Protection Act 2014 (Vic) and the VPDSF. Additional contractual requirements may apply where PlanSuite supports a Victorian public-sector customer.

> **Data return and deletion**
>
> Users may delete properties and uploaded content at any time, and full account or organisation data deletion is actioned on request. On termination, a customer may request export of its data in a standard format within 30 days of the termination date. After that period, data may be deleted unless retention is required by law.

7. Subprocessors & external services

The providers below support hosting, AI processing, mapping, transactional email, in-product support, billing, error monitoring, customer administration, and official

Victorian planning data access. Not every provider processes every customer interaction. This depends on the modules and integrations a council enables.

For each provider the table records where Customer data is processed, where it comes to rest, and from where PlanSuite personnel can reach it. A provider shown as not storing data receives it only for the life of the request. The same register is published as Annex B of the Data Processing Agreement, and both are generated from one source so they cannot drift apart.

Provider	Purpose	Processed in	Stored in	Accessible from
Amazon Web Services	Cloud hosting, database, document storage and application logs	Sydney, Australia	Sydney, Australia	Australia
Google Cloud Vertex AI	AI analysis of property data, planning scheme content and user inputs. Not used for model training.	Global endpoint; may occur outside Australia	Not stored	Australia
Google Maps Platform	Map display, aerial imagery, Street View imagery of the property, and address search	United States	Not stored	Australia
Victorian Government APIs	Official planning and property data (VicPlan, Vicmap, Victorian GeoServer)	Victoria, Australia	Not stored	Australia
Nearmap	Optional high-resolution aerial imagery, enabled per organisation under the council's own Nearmap licence	Australia	Not stored	Australia
Postmark	Transactional email delivery	United States	United States	Australia
Intercom	In-product support messaging	United States	United States	Australia

Provider	Purpose	Processed in	Stored in	Accessible from
Stripe	Subscription billing. Card details are captured by Stripe directly and are not held by PlanSuite.	United States	United States	Australia
Sentry	Application error monitoring. Session replay is captured only when an error occurs, with all text masked and all media blocked.	Germany, European Union	Germany, European Union	Australia
HubSpot	Customer relationship management for account and organisation contact records	United States	United States	Australia
Slack	Internal operational and service notifications to PlanSuite staff	United States	United States	Australia

Supplier governance

PlanSuite remains responsible for the compliance of its subprocessors and will notify customers of material changes to this list under the Data Processing Agreement. A supplier's own certifications do not confer certification on PlanSuite.

8. Monitoring, backups & resilience

- Continuous system monitoring is maintained across production infrastructure.
- Application error monitoring supports rapid detection and diagnosis of faults. Diagnostic session replay is captured only on error, with all text masked and all media blocked, so uploaded plans and applicant details are not captured.
- AWS RDS automated backups provide database recovery with point-in-time recovery.
- AWS S3 object versioning is enabled for document storage in production.
- Backups are encrypted at rest and held within AWS Sydney (ap-southeast-2).

- Production database deletion protection is enabled.
- PlanSuite aims for continuous availability. Our public Terms do not guarantee uninterrupted service.

A documented IT Disaster Recovery Plan and continuity arrangements set out our critical systems, recovery procedures for data loss, availability zone failure, application failure and credential compromise, and the arrangements covering key-person unavailability. Restore validation is performed on a recurring cadence: production data is restored into an isolated instance, restored record counts are verified against the live database, and the recovery time is recorded. Results and any findings are logged against the plan, which is reviewed annually. The plan is available to councils on request.

> **Recovery objectives**
>
> Our recovery point objective is approximately 5 minutes, based on point-in-time recovery with 14 day backup retention. PlanSuite does not publish a contractual recovery time objective, and does not state a production recovery time it has not measured. Council-specific RTO or RPO requirements can be agreed in the applicable contract or service schedule.

9. Incident response & data breach management

Our Data Processing Agreement commits PlanSuite to notifying affected customers within 72 hours of becoming aware of a confirmed data breach affecting customer data. Our incident process operationalises that commitment:

1. Detect and triage the suspected security or privacy incident.
2. Contain the incident and preserve relevant evidence.
3. Assess affected systems, information, customers and likely impact.
4. Eradicate the cause and remediate identified weaknesses.
5. Recover service and validate that controls are operating as expected.
6. Notify affected customers under contractual commitments and applicable law.
7. Complete a post-incident review and track corrective actions to completion.

72-hour commitment and the law

The 72-hour customer notification is a PlanSuite contractual commitment. Australian Notifiable Data Breach obligations are separate: where the Privacy Act NDB scheme applies, suspected eligible breaches are assessed as required by law and confirmed eligible breaches are notified as soon as practicable. The 72-hour commitment is additional to, not a substitute for, applicable law.

10. Essential Eight alignment

Strategy	Status	Basis
1. Application control	ALIGNED	AWS ECS Fargate. Only our verified, containerised application code executes in production, with no general-purpose OS where arbitrary applications could run.
2. Patch applications	ALIGNED	Automated vulnerability scanning of application dependencies raises patch pull requests when a known vulnerability is published. Continuous deployment means fixes reach production quickly.
3. Configure Microsoft Office macros	NOT APPLICABLE	PlanSuite is a browser-based service with no Office macro, ActiveX or downloadable-executable dependency.
4. User application hardening	ALIGNED	The platform does not use Flash, Java applets, browser plugins or web advertising, so the end-user attack surface is minimal by design. Endpoint browser hardening is controlled by the council's own managed environment.
5. Restrict administrative privileges	ALIGNED	Least privilege, AWS IAM restrictions and application RBAC. No long-lived IAM users in the production account, and no root sign-in path: centralised root access management is enabled, the production account holds no root credentials, and root password recovery is blocked.
6. Patch operating systems	ALIGNED	AWS Fargate manages host operating system and security patching. PlanSuite does not operate the host OS.

Strategy	Status	Basis
7. Multi-factor authentication	ALIGNED	Council SSO can enforce MFA through the council identity provider. Internal infrastructure access uses short-lived, role-based credentials issued through an MFA-enforcing identity provider, with no long-lived IAM users in the production account.
8. Regular backups	ALIGNED	RDS automated backups with point-in-time recovery, S3 object versioning, and encrypted backups held in Sydney.

The Essential Eight includes maturity levels that can be independently assessed where required. PlanSuite states alignment and does not claim an independently assessed maturity level. This pack does not assign PlanSuite Maturity Level 1, 2 or 3.

11. Assurance, certifications & audit status

Assurance item	Status	Statement
ASD Essential Eight alignment	CLAIMED	PlanSuite maps the platform against all eight strategies, as set out in section 10.
Independent Essential Eight assessment	NOT CLAIMED	No independent assessment report is held.
ISO/IEC 27001 certification	NOT CLAIMED	No PlanSuite certification is represented in this pack.
SOC 2 report	NOT CLAIMED	No PlanSuite SOC 2 report is represented in this pack.
IRAP assessment	NOT CLAIMED	No PlanSuite IRAP assessment is represented in this pack.
Independent penetration test	NOT CLAIMED	No independent penetration-testing report is represented in this pack.
AWS provider assurance	PROVIDER CAPABILITY	AWS operates extensive security and compliance programs, but AWS certification does not by itself certify PlanSuite.

Transparency principle

PlanSuite provides a certification, audit or penetration-test report only where it holds that artefact and is authorised to disclose it. The absence of a claim here is intentional, and avoids implying certification that has not been evidenced.

12. Shared responsibility for council use

Party	Primary responsibility
PlanSuite	Platform hosting; application security; encryption; PlanSuite access controls; backups; disclosed subprocessors; incident handling for the service.
Council	Identity-provider policy and MFA where SSO is used; user provisioning and deprovisioning; endpoint and browser security; internal information classification; records management; verification of AI-assisted outputs.
Shared	Configuration of SSO and integrations; appropriate uploaded data; incident coordination; privacy handling; supplier review; contractual security requirements.

Contact & evidence requests

We welcome council security, privacy and procurement questions. Councils may request clarification of controls, current subprocessor information, SSO configuration details, data-handling specifics, incident notification arrangements, or any independent assurance artefact PlanSuite holds and is authorised to disclose.

Organisation	PlanSuite Pty Ltd | ABN 57 691 312 795
Security & privacy contact	support@plansuite.com.au
Website	www.plansuite.com.au
Related pages	Security & Data Protection, Essential Eight Compliance, Legal Terms & Policies
Pack issue	Version 1.0 | 30 July 2026

References to external frameworks (ASD Essential Eight, OVIC VPDSF, OAIC Notifiable Data Breaches guidance) indicate alignment or relevance only. They do not represent independent certification, accreditation or assurance unless expressly stated.