Nebula Platform

PRODUCT, SECURITY AND TRUST WHITE PAPER

Product, security and trust white paper

Turn agreements into delivery.

Nebula reads the documents that define the work, builds a shared delivery plan, and applies industry know-how to manage people, money, risk, decisions and evidence throughout the engagement.

Purpose. This paper explains Nebula's product model, current trust posture and the standards that shape its control design. Assurance evidence is matched to a defined product and procurement scope.

What Nebula is A governed engagement workspace that keeps sources, positions, decisions and delivery evidence connected.	**What trust means here** Evidence about who did what, when and with what authority, while uncertainty and disputes remain visible.
Document status Public information paper. Version 1.3, 7 September 2026. Issued by Nebula Platform.	**Revalidation** Product, provider and deployment details are reviewed for the intended procurement scope.

READER GUIDE / NEBULA WHITE PAPER

About this paper

A product and procurement document for organisations assessing how Nebula supports engagement delivery, represents trust and structures security and assurance review.

Intended audience Engagement leaders, commercial teams, procurement, risk, privacy, security, assurance and legal advisers.	**In scope** Product model, engagement lifecycle, standard deployment, security controls, proof, reputation and procurement questions.
Procurement scope Customer architecture, negotiated controls, evidence and approval requirements are assessed against the intended use.	**Evidence basis** Reviewed product source, versioned configuration and authoritative standard-owner sources. Current provider accounts and contracts require separate confirmation.

Contents

Section	Focus	Page
01	Executive summary and trust model	3
02	From source material to governed delivery	4
03	Document intelligence and authority	5
04	Engagement operations across the lifecycle	6
05	Security architecture and data flows	7
06	Access, privacy and classification	8
07	Standards explained and applied	9
08	Proof, verification and contextual reputation	10
09	Procurement checklist	11
10	References, glossary and document control	12

Use and reliance. This paper provides general product information for evaluation. Customer-specific warranties and assurance commitments are established in the applicable terms or order. Each organisation assesses the proposed data, deployment and controls against its obligations and risk appetite.

01 / NEBULA WHITE PAPER

The trust problem Nebula is built to address

Engagements fragment when the documents, people, money, risk, decisions and evidence are managed in separate systems and reconstructed only after something goes wrong.

Nebula is a convener. It creates a shared, source-linked delivery context while preserving each participant's position, the state of any dispute and the authority required for each material effect.

Design commitments

Source before rule Important requirements, dates, money and decisions remain linked to the material that supports them.	**No imposed truth** Source observations, model interpretations, party positions, accepted facts, determinations and disputes remain distinct.
Authority before effect Reading can inform locally. Money, rights, notices, enforcement and reputation follow the authority path for that effect.	**Change preserves history** New documents, guidance and events update the engagement without erasing earlier positions, decisions or completed work.
Evidence earns trust Proof establishes record integrity. Context, evidence and the relevant decision-maker establish the meaning of an event.	**Customer learning stays private** Private customer material is used to provide the service and is not promoted into cross-customer patterns.
Private by design Access is checked against organisation, engagement and role permissions. Recorded audit events name their actors; workflow notifications inform the affected participants.	**Your work is yours** Your work remains yours. Sharing with participants and connected services follows the relevant permissions, not unrestricted access to your organisation's work.

Current standard deployment

Application hosting Containerised Next.js application hosted on Railway (production hosting confirmed on 7 September 2026). The deployed region is not established.	**Operational records** Managed Neon PostgreSQL.
Object storage Managed Cloudflare R2.	**Document intelligence** Code-available AI providers behind one boundary, with a session-bound model and deployment checks.

02 / NEBULA WHITE PAPER

From source material to governed delivery

Nebula treats an agreement, brief, grant, scope, specification, correspondence and delivery evidence as sources for an engagement, not as the boundary of the product.

Stage	What happens	What Nebula preserves
1. Understand	Read sources and guidance; propose requirements, parties, roles, dates, money, risks and unresolved matters.	Provenance, uncertainty and distinct participant positions.
2. Plan	Build the work, dependencies, responsibilities, budgets, evidence needs and decision paths.	A versioned shared delivery plan and the scope of each acceptance.
3. Mobilise	Invite participants, assign owners and connect prerequisites, approvals and resources.	Membership, role, authority and dependency history.
4. Deliver	Coordinate work, claims, notices, risks, questions, files, journals and collaboration.	A current record tied to why each event matters.
5. Adapt	Reconcile new documents, variations, extensions, evidence and real-world events.	Semantic change, earlier state, accrued work and unresolved residue.
6. Close	Resolve deliverables, payment positions, defects, handover, continuing duties and lessons.	Closeout evidence and eligible contextual reputation events.

The anatomy of a trustworthy engagement record

Source
The passage, document, statement or recorded event supporting a proposition.

Position
Who supplied a claim or interpretation and whether another participant accepts, disputes or has not addressed it.

Authority
The role or decision path permitted to cause a particular effect.

Time and dependency
The observed date, freshness state, predecessors and downstream consequences.

Money and risk
The claim, budget effect, exposure or consequence represented by the source and current state.

Evidence and history
Files, responses, confirmations and prior versions retained with their provenance.

Documents and guidance become an engagement model. The model becomes a delivery plan. Approved capabilities then operate that plan through controlled actions, evidence and continuous reconciliation.

03 / NEBULA WHITE PAPER

Document intelligence with an authority boundary

Reading is the start of the engagement model. Code-available AI models propose source-grounded structure while server-owned controls govern what can affect people, money, rights, enforcement or reputation.

Step	Product behaviour	Control
Inventory	Identify source families, revisions and likely relevance.	Missing, superseded or unrelated material remains visible for review.
Interpret	Propose requirements, parties, dates, amounts, relationships and ambiguity with source references.	Model output remains a proposal with confidence separate from authority.
Reconcile	Compare new material, guidance and evidence with the existing engagement state.	Semantic changes and unresolved residue remain explicit.
Simulate	Show expected actions, notices, money effects, conflicts and consequences before activation.	Simulation produces no product writes.
Operate	Compose approved capabilities for reminders, approvals, evidence, reporting and other workflows.	Closed, server-owned writers validate tenancy, authority and permitted transitions.

Boundaries that make the intelligence trustworthy

Prompt boundary
Quoted source material is treated as data for analysis, not as an instruction to the platform.

Cross-party boundary
One participant's statement remains attributable and distinct from another participant's response.

Execution boundary
Models propose semantic actions. They do not generate arbitrary URLs, service names, transition names or request bodies.

Professional boundary
Legal, technical, commercial, regulatory and assurance decision-makers retain their respective jurisdiction.

Nebula makes what is sourced, believed, accepted, disputed, determined and unresolved legible to the people responsible for delivery.

04 / NEBULA WHITE PAPER

Engagement operations across the lifecycle

Nebula's value emerges when planning, commercial control, collaboration, evidence and reputation remain connected throughout the work.

Workspace and collaboration Questions, responses, files, journals, deliverables and decisions scoped to the engagement and its participants.	**Budget and payment** Claims, assessment, GST basis, retention, accepted change and payment events in one commercial record.
Risk and dependency Late inputs, unanswered questions, approval delays and critical dependencies connected to the work they expose.	**Change and reconciliation** Variations, revised sources, extensions, cost, time, authority and participant positions preserved without silent overwrite.
Deadline operation Trusted dates, reminders and configured follow-up, with material actions routed through the applicable control.	**Evidence and closeout** Defects, rectification, handover, final positions, continuing duties and assurance material kept source-linked.
Reporting Current engagement and portfolio views built from the same operating record rather than a separate reporting reconstruction.	**Contextual reputation** Eligible, attributable events presented with role, evidence, proof coverage and dispute or review state.

A practical control loop

Signal	Nebula connects it to	Responsible response
A prerequisite is late	Owner, source, due date, freshness and downstream dependency.	Ask, respond, escalate or record an authorised change.
A claim exceeds the current position	Claimed value, assessed value, retention, accepted changes and budget.	Keep claim and assessment distinct while the authorised role decides.
Closeout evidence is incomplete	Deliverables, defects, handover, final position and continuing dates.	Resolve ownership and acceptance before closeout.

The engagement model is not a one-time reading. Delivery evidence, decisions, progress, claims and exceptions continuously update the working context.

05 / NEBULA WHITE PAPER

Security architecture and data flows

Nebula's standard architecture combines application controls, managed data services and code-available AI-provider paths under shared safeguards.

Component	Deployment detail	Purpose and safeguard
Application hosting	Railway container deployment	Hosts the application and its embedded schedules; the deployed region is not established and none is claimed until verified.
Operational database	Managed Neon PostgreSQL	Stores structured engagement records.
Object storage	Managed Cloudflare R2	Stores documents and files.
Document intelligence	Code-available provider and session-bound model; region follows the selected service	Nebula policy excludes customer-data training. Configured prompt and extracted-text fields use default pattern redaction; filenames and native PDFs are not guaranteed redacted. Provider terms and the deployed setting require confirmation.
Proof records	Polygon and Nebulad paths	Reports each available confirmation state independently. Public Polygon data carries a hash rather than the source document.
End-user access	Customer-controlled devices and networks	Customer endpoint, credential hygiene and network controls remain part of shared responsibility.

Current application controls

Transport and storage
Current provider documentation states that the managed database and object-storage services encrypt data at rest. The deployed boundary, key custody and backup coverage cannot be confirmed from current account or applicable contract evidence. Application responses configure HSTS and named HTTP provider endpoints use HTTPS. Live provider and database transport require verification. Separately, signing keys are wrapped with AES-256-GCM.

Identity and membership
Authenticated sessions, organisation and engagement membership, rate-limited sign-in, TOTP MFA and a separate super-admin gate.

Auditability
The shared authentication gate makes best-effort access-log writes. Defined engagement transitions and selected exports have activity-record paths.

File access
Stored objects use application-controlled access paths. Workspace membership and customer sharing decisions govern access.

The live security page is the current product statement: nebulaplatform.com.au/security

06 / NEBULA WHITE PAPER

Access, privacy and information classification

Purpose-limited data use, attributable access and visible handling context support the Australian privacy and security posture of the standard service.

Organisation and engagement scope Membership and role checks constrain ordinary actions and shared views to authorised participants.	**Administrative scope** Super-admin functions use a separate gate with best-effort attributable administrative audit writes.
Purpose-limited customer content Customer content is processed to provide the service. Nebula policy excludes sale, advertising use and model training; applicable provider terms require confirmation.	**Text redaction** By default, configured prompt and extracted-text fields replace selected Australian identifiers before provider processing. Filenames and native PDF binaries are not guaranteed redacted. The deployed setting requires confirmation.
Correction and erasure Account data can be corrected or anonymised. Shared engagement, audit and proof records follow their evidence, security and legal retention basis.	**Service chain** The disclosed path includes Railway, Neon, Cloudflare, Resend, code-available AI providers, server-proxied weather services and customer-selected webhook destinations where used.

Classification label and authorised environment

Nebula records	Authority decision	Procurement action
UNCLASSIFIED, OFFICIAL, OFFICIAL: SENSITIVE or PROTECTED handling context.	The accountable customer and assurance authority determine environment, personnel access and approval.	Select, assess and authorise controls for the intended information and use.
Customer-specific handling requirements and engagement context.	The customer determines who may contribute, view, decide and share.	Confirm the defined deployment, evidence and operating responsibilities before use.

Nebula is responsible for controls implemented in the service. Customers govern authorised participants, source rights, device and credential hygiene, classification, retention choices and professional decisions.

07 / NEBULA WHITE PAPER

What the standards mean and how Nebula uses them

Reference standards organise control design, evidence and procurement questions around a defined system boundary and intended use.

Reference	What it is	How Nebula uses it
SOC 2	An AICPA attestation examination under the Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy.	The criteria structure relevant control design and evidence.
ASD ISM	The Australian Signals Directorate's cyber security framework and considered advice for systems and information.	Applicable guidance informs the security and data-handling control matrix.
IRAP	A program under which ASD-endorsed assessors assess a defined system against applicable ISM controls.	The system boundary, control mapping and evidence support the assessment path required for a deployment.
Australian Privacy Principles	Thirteen principles under the Privacy Act covering governance, collection, use, disclosure, integrity, access and correction.	Purpose limitation, disclosure, access, correction, governance and accountable handling shape the privacy program.

Reading assurance evidence well

Name the system boundary
Connect any report, assessment or control map to the exact product, deployment and service period.

Name the evidence
Record the criteria, period, exceptions, provider roles and responsible owner supporting the decision.

Match assurance to use
Classification, data flow, enabled capabilities and customer obligations determine the evidence required.

Revalidate change
Providers, regions, controls, subprocessors and intended use can change the decision context.

Nebula maps control design and evidence to reference standards for a defined scope. Procurement decisions remain grounded in the current material for the intended deployment.

08 / NEBULA WHITE PAPER

Proof, verification and contextual reputation

Proof establishes the integrity and timing of a retained record. The relevant evidence, participants and decision authorities establish what the underlying event means.

Layer	Question it can answer	Relevant authority
Source link	Which passage, statement or recorded event supports this proposition?	The authorised reviewer assesses interpretation and relevance.
Attribution	Which authenticated participant supplied, accepted or determined the event?	Organisation authorities confirm delegation and external authority.
Confirmation state	Was the event claimed, accepted, certified, disputed or determined?	The applicable participant or independent decision process.
Cryptographic proof	Does the presented record match the commitment made at that time?	Underlying evidence and authorised people establish business meaning.
Reputation event	Did an eligible event contribute to the organisation's contextual history?	Review and appeal paths preserve corrections, dispute outcomes and context.

A more useful record of how organisations perform

For emerging organisations
Credible delivery history can demonstrate capability beyond brand recognition or self-authored case studies.

For buyers and partners
Recent, role-specific history can support proportionate diligence while the selection decision remains with the buyer.

For an industry
Contextual evidence can reward reliable delivery and make repeated poor conduct harder to hide across fragmented records.

For the organisation assessed
Released views retain event context, proof coverage, dispute state and the applicable review history.

Integrity establishes record consistency. Context, evidence and the authority relevant to each decision establish business truth and professional standing.

09 / NEBULA WHITE PAPER

Procurement checklist

Use this page to match the intended deployment to the sensitivity, assurance and operating needs of a real engagement.

Questions to settle before use

Data Which records and files will enter Nebula? What classification, retention, location and sharing rules apply?	**People** Who can invite participants, approve the delivery plan, decide changes and administer the organisation?
AI Which reading functions and code-available provider paths will be used? What provider terms, redaction setting and review are required for the intended material?	**Authority** Which effects can operate locally, which need relevant participants, and which require a defined decision-maker?
Operations Which dates and external observations are fresh enough to drive workflow? How will stale information be handled?	**Exit and evidence** What must be exported, retained, corrected or erased at closeout? Which continuing duties remain?

Evidence to request and verify

Area	Due diligence evidence
Architecture and location	Current data-flow diagram, provider roles, service regions, object-storage scope and AI processing paths.
Identity and access	Role model, privileged-access process, session controls, joiner and leaver practice, and customer identity options.
Application security	Secure-development process, dependency controls, vulnerability handling and current testing evidence.
Operations	Incident process, backup and recovery arrangements, monitoring responsibilities, continuity assumptions and escalation path.
Privacy and retention	Subprocessor information, cross-border handling, correction and erasure process, proof retention and customer exit.
Assurance	Exact scope and date of the control mapping, assessment material or independent report relied upon for the decision.

A complete procurement decision names the data, users, authority, classification, regions, enabled capabilities and evidence relied upon for the intended scope.

10 / NEBULA WHITE PAPER

References, glossary and document control

Authoritative sources define the standards language used in this paper. Document control keeps the published position attributable and reviewable.

Authoritative references

AICPA, System and Organization Controls: aicpa-cima.com/soc
NIST summary of AICPA Trust Services Criteria: nist.gov/itl/applied-cybersecurity/privacy-engineering/aicpa
Australian Signals Directorate, Information Security Manual: cyber.gov.au/resources-business-and-government/essential-cyber-security/ism
Australian Signals Directorate, IRAP: cyber.gov.au/irap
Office of the Australian Information Commissioner, APPs: oaic.gov.au/privacy/australian-privacy-principles

Glossary

Term	Meaning in this paper
Engagement model	The source-linked representation of participants, requirements, positions, authority, states, money, risk, evidence and history.
Delivery plan	The versioned working plan built from the engagement model, including the scope and attribution of each acceptance.
Position	A statement or interpretation attributable to the participant or system that supplied it.
Verified	A defined confirmation or proof check has succeeded. Its precise meaning depends on the layer being verified.
Proof anchor	A cryptographic commitment used to check record integrity and timing.
Control mapping	A comparison of implemented controls and evidence to reference criteria for a defined scope.

Document control

Field	Value
Document	Nebula Product, Security and Trust White Paper
Version and classification	1.3, issued 7 September 2026 / Public
Issuer	Nebula Platform Pty Ltd / ACN 667 540 025
Copyright	(c) 2026 Nebula Platform Pty Ltd. All rights reserved.
Scope	Standard Nebula product and deployment posture described in this paper
Change note	Hosting, service-chain wording and access explanations updated. Other controls retain their existing evidence dates and limits.
Review trigger	Providers, regions, product controls, standards or assurance evidence change

Current statement and contact: nebulaplatform.com.au/security / security@nebulaplatform.com.au
Nebula convenes the engagement. People retain authority. Evidence earns trust.