Agentic Security Pty Ltd General Terms and Conditions

Version 1.0, effective 9 October 2026

Agentic Security Pty Ltd ACN 701 054 506 (ABN 42 701 054 506) of Perth, Western Australia 6000, which also trades as Cypen and cypen.ai (**Agentic Security**, **Cypen**, **we**, **us**, **our**).

These terms govern platform-delivered Penetration Testing Services and Adversarial Exposure Validation (AEV) Subscription Services for business clients, including Partners testing their own customers' Systems. They are not offered to consumers. Nothing in these terms excludes rights that cannot lawfully be excluded.

Capitalised terms are defined in clause 21.

1. Agreement and applicable terms

1.1 These terms apply to each Proposal, Sales Quotation, Statement of Work, platform order, invoice or payment request that incorporates them, and to every Partner Account.

1.2 An Agreement is formed when the earliest of the following occurs:

(a) the Client signs or accepts a Statement of Work, Proposal, Sales Quotation or platform order;

(b) the Client issues a purchase order and Agentic Security accepts it in writing;

(c) the Client pays all or part of an invoice or payment request for the Services;

(d) Agentic Security commences Services at the Client's written or platform-recorded request; or

(e) the Client accepts these terms through the platform or another acceptance mechanism Agentic Security provides.

Payment is acceptance of the incorporated terms and the order or proposal to which it relates, whether or not separately signed. A person accepting for the Client represents that they have authority to bind it.

1.3 Each Agreement is a separate contract. A test launched within an existing Agreement does not create a separate Agreement unless expressly ordered as one. Clause 16.2 applies per Agreement; the limits in clause 16.3 apply across Agreements.

1.4 Inconsistencies are resolved in this order: an express variation agreed by both parties; the Statement of Work, Proposal, Sales Quotation or platform order; the applicable Schedules; then the general terms. Agreed platform scope settings supplement those documents but do not override an express negotiated restriction unless the change is agreed. For Partner Engagements, clauses 2, 7, 8, 13 and 14.2 of Schedule 3 prevail over other documents and Schedules and may be varied only by a variation signed by both parties expressly identifying the clause varied.

1.5 Client procurement or other terms do not apply unless Agentic Security expressly accepts them in a signed document.

1.6 Schedule 1 applies only to Penetration Testing Services. Schedule 2 applies only to AEV Subscription Services. Schedule 3 applies additionally to Partner Engagements and prevails over other Schedules to the extent of a conflict concerning a Partner Engagement. Schedule 4 applies to both Services.

1.7 The version accepted when an Agreement is formed governs it. Agentic Security may publish updated terms for acceptance on a new engagement, renewal or new test launch. Express acceptance by an authorised user applies the updated version prospectively to that engagement, renewal or test and its resulting findings and fieldwork. For a test within an existing subscription, the agreed price, expiry, asset allowance and Australian processing requirement remain unchanged unless expressly varied. Earlier work and automatically continuing tests remain subject to their applicable accepted version. Agentic Security will record the accepted version and comply with update-notice requirements imposed by Law or expressly agreed with the Client.

2. Scope and Rules of Engagement

2.1 Testing requires an agreed scope identifying the targets, permitted period or subscription term, methods and exclusions, relevant contacts and arrangements to stop testing. Scope and Rules of Engagement may be recorded in the Proposal, Statement of Work, Sales Quotation, platform order or approved platform settings.

2.2 Agentic Security will test only authorised, in-scope targets.

2.3 Unless expressly included in the agreed scope, Services exclude:

(a) denial-of-service testing and load or stress testing intended to cause service degradation or failure;

(b) exploitation intended to destroy, encrypt, corrupt or permanently alter data or make a System unrecoverable;

(c) social engineering;

(d) physical intrusion or premises testing;

(e) testing third-party Systems without the authorisation required by clause 5.2; and

(f) testing the Client's people rather than its Systems.

2.4 An approved domain, subdomain, hostname or URL includes the addresses and hosts through which it resolves using DNS, including CNAME records and chains, for testing that approved target. Clause 5.2 applies to them. This does not authorise testing unrelated services or other tenants on that infrastructure. Where Agentic Security identifies a shared or multi-tenant provider, testing remains limited to the approved hostname; testing the underlying infrastructure independently requires separate scope approval and authority. DNS association alone does not approve a newly discovered asset under Schedule 2.

2.5 If a target is not covered by the agreed scope or clause 2.4, Agentic Security will seek the Client's explicit approval before testing it. Approval may be given through the platform or another agreed written mechanism.

2.6 Scope changes take effect only when agreed through the platform or in writing. Any additional fees must be agreed as a fixed price or purchased subscription capacity before the additional work begins.

2.7 Penetration testing may run at any hour within its booked window unless agreed restrictions apply. AEV operates throughout the subscription term, including nights, weekends and public holidays, at the agreed testing frequency and subject to scope, pauses and service availability.

2.8 The Client acknowledges that authorised testing may alter or lose data, affect accounts or configuration, interrupt services, consume resources, or trigger workflows and communications.

2.9 The Client accepts the inherent operational risks of authorised testing, including testing production Systems, subject to clauses 15 and 16. The Client must assess those risks, maintain the recovery capability in clause 4(c), and restore its Systems and data when needed.

3. Service delivery and findings

3.1 Agentic Security will perform the Services with the skill, care and diligence reasonably expected of a competent professional provider of cyber security testing services.

3.2 Testing is performed through Agentic Security's platform and agents, with human oversight and review by Personnel with appropriate qualifications and experience.

3.3 Agentic Security will comply with applicable Laws and the Client's reasonable security, access and safety policies notified before work begins.

3.4 Agentic Security will deliver the Deliverables specified in the Agreement.

3.5 For direct Clients, findings are reviewed and triaged by Agentic Security before being made available as client findings or included in a report. The Client remains responsible for prioritising remediation, assigning responsibility and acting on findings. For Partner Engagements, the Partner performs review, validation, triage and publication under Schedule 3.

3.6 Where Agentic Security identifies a vulnerability it reasonably assesses as critical, or evidence of an existing or previous compromise (a **Critical Finding**), it will notify the direct Client's nominated escalation contact without undue delay and within 24 hours of identification. Schedule 3 clause 10.2 sets out the different arrangement for Partners.

3.7 Agentic Security will use good-faith professional judgment to select proportionate steps to validate findings and demonstrate impact within the agreed scope. It will take reasonable steps to minimise unnecessary data extraction and disruption, will not deliberately carry out destructive activities excluded by clause 2.3(b), and will not use obtained access for purposes unrelated to the engagement. It will not establish persistence beyond the authorised testing period.

3.8 On an authorised direction to stop testing, Agentic Security will stop as soon as it is safe to do so. Penetration-test scheduling consequences are governed by Schedule 1; AEV pauses are governed by Schedule 2 and do not extend the subscription term.

3.9 Where testing reveals evidence of third-party compromise, Agentic Security will preserve relevant fieldwork and suspend affected testing where continuing could destroy evidence or interfere with the Client's response. It will escalate under clause 3.6, subject to the Partner exception. The Client is responsible for

its incident response and legal notifications. Agentic Security will not notify third parties except as required by Law, directed by the Client, or permitted in relation to Unauthorised Testing under Schedule 3.

3.10 Findings and severity ratings reflect Agentic Security's professional judgment. Reports do not certify security or compliance.

3.11 Agentic Security will make reasonable efforts to minimise and, where feasible, remove changes and testing material it introduces into the Client's Systems. It will identify known remaining items and recommended cleanup actions in reports or through the platform on a reasonable-efforts basis. The Client is responsible for final cleanup and restoration.

4. Client responsibilities

The Client must:

(a) provide accurate scope information and disclose known operational sensitivities and dependencies;

(b) provide and maintain the agreed access, credentials and supporting information needed for testing;

(c) maintain appropriate, verified backups and a tested restoration capability for the in-scope Systems before and throughout testing, including ongoing AEV testing;

(d) nominate technical and escalation contacts with arrangements to receive urgent communications during the authorised testing period;

(e) manage, at its cost, alerts, incident responses and third-party charges arising within its environment from authorised testing;

(f) respond to reasonable requests and decisions within agreed timeframes; and

(g) keep its scope approvals and permissions current and promptly disable affected targets and notify Agentic Security if testing authority is withdrawn or becomes insufficient.

5. Authorisation

5.1 The Client authorises Agentic Security, its platform and authorised operators to access and test the in-scope Systems using the agreed methods during the authorised period.

5.2 For each target it submits, approves or enables, the Client represents and warrants that it:

(a) owns or controls the target or holds sufficient current authority from its owner or operator;

(b) has obtained all required third-party consents, approvals and authorisations and given all required notices;

(c) complies with applicable third-party testing and acceptable-use requirements;

(d) is not authorising testing prohibited by Law, contract, licence or another person's rights; and

(e) has verified that its permissions cover the target and agreed testing.

5.3 The warranties in clause 5.2 apply when the Agreement is formed and each time the Client submits, confirms, enables or changes a target or scope, including through platform controls.

5.4 Agentic Security may rely on the Client's scope and confirmations without independently verifying ownership, third-party restrictions or the sufficiency of permissions. It may request evidence but does not assume the Client's responsibility by requesting or reviewing it.

5.5 In performing the Services, Agentic Security acts as the Client's agent for the authorised testing and is a party to communications on the Client's Systems that it intercepts in that work.

5.6 The Client indemnifies Agentic Security and its Personnel against Loss arising from inaccurate scope information or a breach of clause 5.2, including third-party claims caused by testing the Client was not entitled to authorise. Clause 16.7 applies.

5.7 Agentic Security may decline, suspend or stop testing where it reasonably believes authorisation is absent, invalid, withdrawn or insufficient, without liability for that action subject to clauses 15.6 and 16.7. The Client remains responsible for applicable fees. On request, Agentic Security will give reasons. If its belief is shown to have been incorrect, it will reschedule affected penetration testing without charge and will not apply a scheduling fee for that suspension. Schedule 3 provides additional Partner remedies.

6. Fees and client-side costs

6.1 Fees are the fixed prices for the agreed penetration-test scope or subscription allowance stated in the Agreement. Additional scope or capacity requires agreement under clause 2.6. Partner fees and credits are governed by Schedule 3 clause 14.

6.2 Fees exclude GST and other Taxes, which are payable with the underlying amount.

6.3 The Client is responsible for usage, licence and other charges incurred in its own environment through authorised testing.

7. Invoicing and payment

7.1 Invoicing follows Schedule 1 for direct Penetration Testing Services, Schedule 2 for direct AEV Subscription Services, and Schedule 3 clause 14 for Partner Engagements.

7.2 Invoices are payable within 14 days of the invoice date, using the payment method specified in the invoice or platform order.

7.3 Interest accrues daily on overdue amounts at 4% per annum above the Reserve Bank of Australia cash rate target from the due date until payment.

7.4 The Client must identify an invoice dispute and its reasons within 10 Business Days of receipt and pay the undisputed balance by the due date.

7.5 Except for a properly disputed amount, the Client may not withhold, set off or deduct an amount from payment, to the extent permitted by Law.

7.6 Once an undisputed invoice is seven days overdue, Agentic Security may give seven days' notice of suspension. If it remains unpaid at the end of that notice, Agentic Security may suspend Services and withhold undelivered Deliverables until paid. Payment obligations continue. A direct Client's Critical Finding will not be withheld because of non-payment; Schedule 3 clause 10.2 governs Partner findings.

8. Term

8.1 An Agreement starts under clause 1.2 and continues for its stated term or until the agreed Services are complete, subject to termination. AEV subscription access, expiry and renewal are governed by Schedule 2; unfinished or paused testing does not extend that term.

8.2 These general terms apply while an Agreement remains in force and afterwards to the extent stated in clause 9.5.

9. Termination and consequences

9.1 Either party may terminate by notice if the other commits a material breach that cannot be remedied, fails to remedy a remediable material breach within 14 days of notice, suffers an Insolvency Event, or is prevented from performing by a Force Majeure Event for at least 60 continuous days.

9.2 A Client may terminate Penetration Testing Services for convenience on 30 days' notice. It must pay for Services performed, non-cancellable engagement commitments and applicable Schedule 1 scheduling fees, without double recovery. For a fixed-price engagement, performed work is valued reasonably by reference to the completed proportion of the agreed scope, capped at its agreed price.

9.3 Agentic Security may terminate immediately by notice if testing authority expires, is withdrawn or is invalid, or continuing would reasonably expose it to illegality or legal or personal risk. Schedule 3 provides additional rights for Partner Engagements.

9.4 When an Agreement ends, Services stop and accrued payment obligations remain. On request, Agentic Security will provide completed reports and an available summary of findings to that date, subject to outstanding payment. That condition does not apply to direct Critical Findings or termination for Agentic Security's material breach. Schedule 2 clause 6 and Schedule 3 clause 12.4 govern post-service report availability. Confidential information and retained fieldwork remain governed by clauses 10 to 13.

9.5 Termination does not affect accrued rights or liabilities. Clauses 3.11, 5.2 to 5.6, 7.2 to 7.5, 9.4 to 17.3 and 20 to 21; Schedule 1 clauses 3.2 to 3.4, 4.3 and 6; Schedule 2 clause 6; and Schedule 3 clauses 1.3, 6 to 10 and 12 to 15 survive to the extent relevant, together with provisions that by their nature are intended to continue.

10. Confidentiality

10.1 A party receiving Confidential Information must use it only for the Agreement, protect it with at least the care used for its own confidential information and no less than reasonable care, keep it confidential, and promptly notify the other party of suspected unauthorised access or disclosure. On request or termination it must return or destroy the information, subject to clause 10.4 and the retention arrangements in clause 13.

10.2 Disclosure is permitted to Personnel, professional advisers and insurers who need the information and are bound by confidentiality; to providers as disclosed under clauses 11 and 19 and Schedule 4; as expressly permitted by the Agreement; or as required by Law, a court or regulator. Where lawful and practicable, the disclosing party will give advance notice of a compulsory disclosure.

10.3 These obligations do not cover information already lawfully held without restriction, independently developed without using the other's Confidential Information, or publicly available other than through a breach.

10.4 Information may be retained where required by Law or reasonably necessary for insurance or legal records. Inaccessible backup or

archive copies may remain where selective deletion is not reasonably practicable, subject to applicable privacy duties, restricted use and ordinary retention cycles. Retained information remains protected.

10.5 The identification licence in clause 14.7 does not permit disclosure of an engagement's scope, dates, findings or other details, or publication of a case study or testimonial, without prior consent.

10.6 Confidentiality obligations continue indefinitely.

11. Privacy and processing locations

11.1 Agentic Security handles Personal Information in accordance with the Australian Privacy Principles and undertakes to do so whether or not it is an APP entity under the Privacy Act. Its privacy policy is available at https://cypen.ai/privacy.

11.2 The Client must obtain and maintain the permissions and notices required by Privacy Laws for the collection, access, use and handling of Personal Information through the Services.

11.3 Agentic Security will collect and use Personal Information only as reasonably necessary to perform the Services and for permitted purposes described in clause 13. It will use professional judgment to minimise extraction and will mask, redact or truncate it in reports and model inputs where reasonably practicable without defeating the testing or evidentiary purpose.

11.4 Each party will promptly notify the other of a Security Breach affecting its data and reasonably assist with assessment, containment and response, including legally required breach assessments and notifications.

11.5 The Client must identify Australian processing requirements before the affected Services begin. Where the Agreement records an Australian-only requirement, Agentic Security will configure engagement storage, testing workloads and model inference to remain in Australia, with access to engagement content restricted to authorised operators in Australia. Any exception requires express agreement before the affected processing. Without that requirement, the Client authorises the Australian and overseas processing disclosed in Schedule 4, subject to applicable privacy obligations.

11.6 Australian-only engagement requirements apply to engagement processing. Business administration and development use the locations and information categories in Schedule 4, unless otherwise expressly agreed. Agentic Security will limit information supplied to those systems to their stated purposes and the agreed residency requirements.

11.7 Agentic Security may update the provider list through the acceptance process in clause 1.7, subject to notice or approval required by Law or expressly agreed with the Client. Agreed residency and confidentiality obligations continue to apply.

12. Security

12.1 Agentic Security maintains reasonable technical and organisational controls to protect Client Data and Engagement Fieldwork.

12.2 Agentic Security's current security controls are described in its Trust Centre at https://cypen.ai/trust.

12.3 Agentic Security will take reasonable measures within its control to prevent a Security Breach and notify the Client without undue delay if one affects its data or Confidential Information.

12.4 On reasonable request, once in any 12-month period without charge, Agentic Security will provide evidence of these controls and respond to the Client's security questionnaire.

13. Engagement Fieldwork and credentials

13.1 Engagement Fieldwork means material retained in carrying out and documenting Services, including scope and approval records, reports, inventories, models, investigation notes, evidence and raw testing output.

13.2 Agentic Security will securely delete client-supplied access credentials from active credential stores when the relevant engagement or subscription ends, or sooner when no longer needed. The Client should revoke or rotate supplied access when testing ends. Credentials embedded in captured evidence are retained and protected under clauses 13.3 to 13.5.

13.3 Agentic Security will retain necessary Engagement Fieldwork for seven years from completion or termination of the penetration-testing engagement, or expiry or termination of the AEV subscription, for Services and continuity for that Client and legitimate professional, insurance and legal records. It will destroy or de-identify information earlier where required by Privacy Laws and delete fieldwork at the end of the retention period, subject to lawful holds or required retention.

13.4 Agentic Security will restrict access to and use of raw fieldwork and take reasonable steps to protect sensitive content and destroy or de-

identify it where required by Law. Backups and archives are governed by clause 10.4.

13.5 The Client may request earlier deletion of fieldwork. Agentic Security will act on the request within 30 days, except for material it must retain or reasonably needs for a lawful claim, investigation or permitted record-keeping purpose. It will explain any retained category and reason.

13.6 Agentic Security may reuse general methods, techniques and lessons to improve its platform only where they contain no Client Confidential Information and do not identify the Client, its Systems, people or data. Agentic Security will exclude Client Data and Engagement Fieldwork from model training.

13.7 Agentic Security may disclose Client Data and client-specific fieldwork only as permitted by the Agreement or Law and must maintain their confidentiality, security and agreed processing location.

14. Intellectual property and reports

14.1 Each party retains its Background IP. Nothing in the Agreement transfers it.

14.2 On full payment under the relevant Agreement, ownership of Intellectual Property Rights in reports and other identified Deliverables passes to the Client, subject to clause 14.3.

14.3 Agentic Security retains its platform, software, agents, methodologies, templates and other reusable intellectual property. Where embedded in a Deliverable, the Client receives a perpetual, worldwide, non-exclusive, royalty-free licence to use that material as part of the Deliverable. Agentic Security may continue using its own material, subject to confidentiality.

14.4 Subject to payment, the Client may share complete, unaltered reports, including their limitations, with professional, regulatory and commercial recipients for legitimate business purposes under confidentiality obligations. Publishing a report, using it in marketing or sharing extracts requires Agentic Security's prior written consent. Partner report rights are set out in Schedule 3 clause 10.

14.5 Reports are not certifications, accreditations or attestations of security or compliance. The Client must not represent them, or use Agentic Security's name, as such.

14.6 Third Party Material is supplied subject to its licence terms and, to the extent permitted by Law, as is and subject to clause 15.4.

14.7 The Client grants Agentic Security a non-exclusive, non-transferable, royalty-free licence to identify it as a client using its name and logo in business and marketing materials. The Client may withdraw this licence by written notice. Agentic Security will remove the identification from materials within its control within 20 Business Days, but need not recall materials already distributed or submitted. Withdrawal does not affect earlier permitted use.

14.8 Identification under clause 14.7 does not permit claims of certification or assurance, or disclosure restricted by clause 10.5. End Client publicity is governed by Schedule 3 clause 15.

14.9 Where a human author contributes copyright material to a Deliverable, Agentic Security will use reasonable endeavours to obtain consent, to the extent permitted by the Copyright Act 1968 (Cth), to the Client's use and modification of the Deliverable without attribution and in ways that would otherwise infringe that author's moral rights.

15. Warranties and service limitations

15.1 Each party warrants that it has authority to enter into and perform the Agreement and that it is binding on it.

15.2 A Client contracting as trustee warrants that it also contracts in its own right, is the sole current trustee, has authority under the trust deed and a full right of indemnity from trust assets, and will provide the deed on request. Otherwise, it warrants that it is not contracting as trustee.

15.3 Agentic Security will perform to the standard in clause 3.1 and the Services will conform in all material respects to the agreed scope.

15.4 Except as expressly agreed and to the extent permitted by Law, Agentic Security does not warrant that testing will identify every vulnerability, that Systems are secure or compliant, that they will withstand attack, or that testing will have no operational impact.

15.5 The Client warrants that information supplied for the Services is materially accurate and complete. Agentic Security may rely on it without independent audit or verification.

15.6 Nothing excludes, restricts or modifies a right, guarantee or remedy that cannot lawfully be excluded, including under the Australian Consumer Law. Where limitation is lawful, liability for breach of such a guarantee is limited, at Agentic Security's option, to resupply or the cost of resupply.

15.7 Findings, severity ratings and recommendations are advisory. The Client decides how to prioritise and implement remediation and is responsible for its resulting business and

technical decisions. Agentic Security does not remediate or secure the Client's Systems unless expressly agreed.

16. Liability

16.1 Agentic Security indemnifies the Client against direct Loss from a third-party claim that a Deliverable as supplied infringes Intellectual Property Rights. This excludes Loss caused or contributed to by modification by others, use outside the Agreement, Third Party Material, breach of a third-party licence or failure to mitigate. The Client must notify Agentic Security promptly and allow it to control the defence and settlement.

16.2 Subject to clauses 16.3 and 16.4, Agentic Security's total aggregate liability arising out of an Agreement, in contract, tort (including negligence), statute or otherwise, is limited to fees paid under that Agreement in the 12 months before the event giving rise to Loss, and in any event to $250,000.

16.3 The following liabilities instead have these limits, to the maximum extent permitted by Law:

Liability	Aggregate limit
Death or personal injury caused by Agentic Security	$10,000,000
Tangible property damage caused by Agentic Security's negligence	$10,000,000
Breach of confidentiality or a Security Breach of Agentic Security's Systems	$250,000
The IP indemnity in clause 16.1	$2,000,000

Each limit applies across all Agreements between the parties and is not cumulative with clause 16.2 or another limit in this clause.

16.4 These limits do not limit liability that cannot lawfully be limited, Agentic Security's fraud or wilful misconduct, the Client's payment obligations, or Partner liability under Schedule 3 clause 8.

16.5 Neither party is liable for indirect or consequential Loss, lost profit, revenue, business, production, goodwill, reputation or opportunity, or loss or corruption of data, however arising. This does not limit payment obligations, liability under clause 5.6 or 16.1, Partner liability under Schedule 3 clause 8, or rights preserved by clauses 15.6 and 16.4.

16.6 Subject to clauses 15.6 and 16.7, the Client indemnifies Agentic Security against Loss arising from:

(a) breach of the authorisation warranties in clause 5.2;

(b) failure to maintain the backups and restoration capability required by clause 4(c), to the extent that failure causes or increases the Loss;

(c) breach of applicable third-party terms or testing restrictions; or

(d) third-party claims arising from data changes or automated processes triggered by authorised testing.

16.7 Liability is reduced to the extent the other party's act, omission or breach caused or contributed to the Loss. Neither party is liable for Loss the other could reasonably have mitigated. No loss may be recovered twice under overlapping provisions.

16.8 A claim requires written notice with reasonable particulars within 12 months after the claimant becomes aware, or ought reasonably to become aware, of the relevant circumstances, and no later than three years after the relevant Services. This restriction does not apply to clause 16.4 liabilities, payment obligations or rights that cannot lawfully be limited.

17. Insurance

17.1 Agentic Security will maintain, during the Agreement and for three years after completion, professional indemnity insurance of at least $2,000,000 per claim, public liability insurance of at least $10,000,000 per occurrence, and cyber liability insurance of at least $250,000 in aggregate.

17.2 Agentic Security will provide certificates of currency on reasonable request.

17.3 Insurance does not change contractual liability limits or exclusions.

18. Platform access

18.1 Where platform access is included, the Client receives a non-exclusive, non-transferable right to use it during the applicable access period for the agreed users and purposes. Direct Clients may use it for their internal business purposes; Partners may use it as permitted by Schedule 3. Access may be suspended or ended only as permitted by the Agreement.

18.2 The Client must secure accounts, use individual named-user accounts and promptly report suspected unauthorised access. It is responsible for actions through its authorised users and must ensure they have appropriate authority for scope, purchasing and acceptance decisions.

18.3 The Client must not attack the platform, bypass access controls, reverse engineer it,

impose unreasonable load, use unauthorised interfaces, store unrelated material or use it unlawfully. Resale, sublicensing and third-party access are prohibited except as expressly permitted for Partners.

18.4 The platform is provided on an as-available basis without a guarantee of uninterrupted access. Agentic Security may suspend it for maintenance and will use reasonable endeavours to give advance notice of scheduled maintenance.

18.5 Agentic Security may immediately suspend a user's access on reasonable suspicion of breach of clauses 18.2 or 18.3 and will notify the Client.

18.6 All platform Intellectual Property Rights remain with Agentic Security. Ownership of Deliverables does not transfer platform rights.

19. Artificial intelligence and providers

19.1 The Client authorises Agentic Security to use AI systems and agents to deliver the Services and process Client Data as described in this clause and Schedule 4.

19.2 Agentic Security uses its own systems and the providers disclosed in Schedule 4. Provider permissions and changes are governed by clauses 1.7 and 11.7. Agreed Australian requirements govern provider selection under clause 11.5.

19.3 For model inference involving Client Data, Agentic Security will use arrangements that prohibit training on inputs and outputs, provide zero retention beyond transient processing, and comply with agreed residency requirements. These requirements apply to intermediaries and downstream model providers.

19.4 Agentic Security reviews and triages direct-client findings under clause 3.5. Partners review and publish findings under Schedule 3.

19.5 Agentic Security remains responsible for its platform's conduct and output under the Agreement and does not transfer that responsibility to an AI or infrastructure provider. Partner responsibility for its own review, edits and publication remains governed by Schedule 3.

19.6 Agentic Security applies the agreed scope and Rules of Engagement to its agents and maintains technical and procedural controls designed to prevent out-of-scope and excluded activity.

19.7 The Client may specify Australian data sovereignty requirements before Services begin. Agentic Security will record the agreed processing configuration and any price or timing effect in the Agreement. Agreed Australian processing requirements will be met through Australian deployment and inference routes.

20. General provisions

20.1 Notices. Formal notices must be emailed to the Client's nominated address or, for Agentic Security, to info@cypen.ai. Breach, dispute, claim and termination notices should use the subject line "Legal Notice"; omission does not invalidate the notice. Notices are received on the next Business Day unless delivery fails. Notice periods run from receipt.

20.2 Disputes. Agentic Security and the Client must attempt to resolve disputes in good faith. If a dispute remains unresolved 20 Business Days after notice, both must attempt mediation in Perth under the Resolution Institute's rules before commencing proceedings. If a mediator cannot be agreed within 21 days after referral to mediation, either may ask the Resolution Institute to appoint one. Either may seek urgent injunctive or interlocutory relief.

20.3 Governing law. Western Australian law applies. The parties submit to the non-exclusive jurisdiction of its courts and competent appeal courts.

20.4 Force majeure. A party is not liable for delay or failure caused by a Force Majeure Event, except for payment obligations, provided it promptly notifies the other and reasonably seeks to resume performance.

20.5 Assignment. Assignment or novation requires the other's consent, except that Agentic Security may transfer the Agreement to an acquirer of all or substantially all of its business on notice.

20.6 Relationship. The parties are independent contracting parties. No partnership, employment, joint venture or agency arises except the limited testing agency in clause 5.5.

20.7 Severability. An unenforceable provision will be read down or severed to the necessary extent; the remainder continues.

20.8 Variation. Variations require express agreement recorded in writing, including an authorised electronic acceptance, except where these terms expressly permit another mechanism. Clause 1.7 governs acceptance of updated terms. The specially protected Partner provisions in clause 1.4 retain their express-signature requirement.

20.9 Waiver. A waiver must be in writing. Delay or failure to exercise a right is not waiver.

20.10 Entire agreement. The Agreement supersedes prior discussions and representations about its subject matter, subject to rights that cannot lawfully be excluded.

20.11 Execution. Agreements may be executed in counterparts or by electronic signature. Express platform acceptance is effective as provided in clause 1.

20.12 Non-exclusive. Either party may provide or obtain similar services elsewhere, including from competitors.

20.13 Third parties. Agentic Security's Personnel may enforce provisions expressly benefiting them, including clause 5.6, and Agentic Security may enforce them on their behalf. No other non-party, including an End Client, has contractual enforcement rights, subject to Law.

21. Definitions and interpretation

21.1 Definitions

AEV or **Adversarial Exposure Validation** means agentic validation of security exposure through discovery and testing of approved external attack-surface assets, provided under Schedule 2.

AEV Subscription Services means the subscription access and adversarial exposure validation described in Schedule 2 and the Agreement.

Agentic Security means Agentic Security Pty Ltd ACN 701 054 506, also trading as Cypen and cypen.ai; those names identify the same entity.

Agreement means the contract formed under clause 1.2, including its accepted order, Statement of Work, Proposal or Sales Quotation, agreed Rules of Engagement and platform scope records, these general terms and applicable Schedules, as validly varied.

Australian Consumer Law means Schedule 2 to the Competition and Consumer Act 2010 (Cth) and its State and Territory applications.

Authorisation Attestation means the Partner's confirmation of sufficient current End Client Authorisation, made by submitting, confirming or enabling a target through its Partner Account under Schedule 3 clause 5.

Background IP means Intellectual Property Rights owned or licensed by a party, developed independently of or before the Services.

Business Day means a day other than a Saturday, Sunday or public holiday in Perth, Western Australia.

Client means the entity engaging Agentic Security, including a Partner.

Client Data means information supplied by the Client or accessed on its Systems in providing Services, including Personal Information and confidential content, whether or not retained as Engagement Fieldwork. Routine business contact and billing information is described separately in Schedule 4 and remains protected by applicable privacy and confidentiality obligations.

Confidential Information means confidential information disclosed or accessed in connection with the Agreement, including Client Data, Engagement Fieldwork, findings, business and technical information, pricing and the Agreement's terms, excluding information described in clause 10.3.

Critical Finding has the meaning in clause 3.6.

Deliverables means reports and other materials expressly identified for delivery under the Agreement.

End Client means a Partner's customer whose Systems, or Systems for which it is responsible, are tested or discovered through a Partner Account.

End Client Authorisation has the meaning in Schedule 3 clause 4.1.

Engagement Fieldwork has the meaning in clause 13.1.

Force Majeure Event means an event beyond reasonable control, including natural disaster, epidemic, war, terrorism, external industrial action or utility or telecommunications failure.

Gross Negligence means serious disregard of or indifference to an obvious risk of harm, exceeding a failure to exercise reasonable care.

GST has the meaning in the A New Tax System (Goods and Services Tax) Act 1999 (Cth).

Insolvency Event means insolvency, a statutory presumption of insolvency, appointment of an external administrator or receiver, a general arrangement with creditors, winding up other than solvent reconstruction, or a substantially equivalent event in any jurisdiction.

Intellectual Property Rights means rights in copyright, trade marks, designs, patents, circuit layouts, trade secrets, know-how and confidential information, registered or unregistered.

Laws means applicable legislation, regulations, mandatory codes, common law, equity and binding orders in the jurisdictions relevant to the Services and in-scope Systems.

Loss means loss, liability, cost, expense or damage, including reasonable legal costs.

Partner means a Client designated by Agentic Security as a partner and provisioned with a Partner Account to deliver Services for End Clients.

Partner Account means the separate partner account, organisation and dashboard provisioned through the platform.

Partner Engagement means Penetration Testing Services or AEV Subscription Services performed through a Partner Account for an End Client.

Penetration Testing Services means the scoped testing engagements described in Schedule 1.

Personal Information and **Privacy Act** mean, respectively, personal information as defined in the Privacy Act 1988 (Cth), and that Act.

Personnel means a party's human employees, officers, contractors and representatives.

Privacy Laws means the Privacy Act and other applicable Laws governing Personal Information.

Proposal and **Sales Quotation** mean the corresponding offer documents issued by Agentic Security incorporating these terms.

Rules of Engagement means the agreed testing scope, methods, exclusions and operational constraints recorded as described in clause 2.1, including relevant platform settings.

Security Breach means unauthorised access to, use, disclosure, alteration or loss of data for which a party is responsible.

Services means the Penetration Testing Services and/or AEV Subscription Services purchased under an Agreement.

Statement of Work or **SOW** means a service description expressly agreed by both parties.

Systems means information technology systems, applications, infrastructure, accounts and services included in or relevant to the agreed scope.

Taxes means GST and other taxes or charges on the supply, excluding taxes on Agentic Security's income or payroll.

Term means the duration of the relevant Agreement under clause 8 and the applicable Schedule.

Third Party Material means third-party proprietary material supplied or made available with the Services.

Unauthorised Testing has the meaning in Schedule 3 clause 7.1.

21.2 Interpretation

Days are calendar days unless stated as Business Days. Amounts are Australian dollars unless otherwise agreed. Writing includes electronic records. References to Laws include amendments and replacements; references to documents mean their validly varied versions, subject to clause 1.7. A person includes a legal entity and its lawful successors. Singular includes plural; "including" is not limiting. Joint obligations bind each obligor jointly and severally.

Schedule 1: Penetration Testing Services

1. Application

1.1 This Schedule applies to Penetration Testing Services purchased as a defined engagement. Schedule 3 governs Partner Engagements where its provisions differ.

1.2 Penetration testing simulates attacker behaviour against the agreed Systems during the booked window. It is a point-in-time assessment subject to the risks and limitations in the general terms.

2. Environment readiness

2.1 The Client must make the agreed environment and access available and maintain their agreed state during the booked window. Material changes affecting scope or the ability to test must be agreed under general clause 2.6.

2.2 Where a representative non-production environment is available and suitable for the agreed assessment, the Client will provide it in preference to production unless the scope requires production testing.

3. Scheduling, rescheduling and delay

3.1 A booked testing window reserves delivery capacity for the agreed engagement.

3.2 If the Client postpones, cancels or reduces a booked engagement, Agentic Security may charge the following percentage of the fixed engagement fee, excluding Taxes:

Notice before the window starts	Postponement	Cancellation or scope reduction
At least 5 Business Days	Nil	15%
Fewer than 5 Business Days	15%	35%

3.3 Where unavailable or unsuitable agreed access or environment prevents testing, Agentic

Security may, at its discretion, charge 10% of the fixed engagement fee, excluding Taxes, per full booked day lost, or apply the postponement fee in clause 3.2. Fractional days are not charged. Only one of those fees may apply to the same delay.

3.4 Agentic Security may reduce or waive a scheduling or delay charge at its discretion. A waiver on one occasion does not waive a later entitlement. Charges must not recover the same loss twice.

3.5 Agentic Security may reschedule by notice and will use reasonable endeavours to give advance notice and agree a suitable replacement window. Client postponement charges apply only to Client-requested changes.

3.6 A Client direction to halt testing may be treated as postponement or cancellation of the affected booked capacity under clause 3.2, except where the halt is reasonably required by Agentic Security's material breach or general clause 5.7 requires rescheduling without charge.

4. Invoicing and early termination

4.1 Direct engagements are invoiced 50% on formation of the Agreement and 50% on delivery of the final report, unless the Proposal or other accepted order specifies a different payment schedule, including 100% on final report delivery. General clause 7 governs payment deadlines.

4.2 Where the agreed payment schedule requires an upfront instalment, Agentic Security may make commencement and reservation of a testing window conditional on receipt of that instalment. Clause 3 may apply if late payment causes an already booked window to be lost.

4.3 If a direct engagement ends before report delivery, any initial instalment is applied to performed Services valued under general clause 9.2 and other amounts properly due, including applicable scheduling charges without double recovery. Agentic Security will refund any excess within 30 days.

5. Reporting

5.1 Agentic Security will deliver the final report on completion of testing.

5.2 Within 5 Business Days of receiving the report, a direct Client may identify factual inaccuracies or relevant context and request correction. Agentic Security will consider the request in good faith and revise the report where appropriate. Decisions on findings and severity remain Agentic Security's professional judgment. Partner review and correction are governed by Schedule 3 clause 10.

5.3 The Client is responsible for assessing and testing proposed remediation and deciding whether and how to implement it.

6. Retesting

6.1 Where the Agreement includes retesting for a direct engagement, one retest engagement is included at no additional charge within 90 days after the final report. The Client may select any or all findings from that report for a single submitted retest batch. Partner retesting is paid under Schedule 3 clause 10.7.

6.2 Retesting is limited to verifying remediation of the selected original findings.

6.3 Retesting outside the included entitlement requires a separately agreed fixed fee.

Schedule 2: Adversarial Exposure Validation (AEV) Subscription Terms

1. Application

1.1 This Schedule governs AEV Subscription Services: platform-delivered agentic AEV for the approved external attack surface during the subscription, subject to agreed frequency, scope and availability. General terms and, for Partners, Schedule 3 apply.

2. Onboarding and asset allowance

2.1 The subscription starts on the date specified in the accepted order or platform purchase confirmation.

2.2 The accepted order or platform purchase confirmation specifies the asset types, counting rules, purchased allowance and annual price.

2.3 The Client may change approved assets within the purchased allowance, subject to authorisation and agreed settings. Increasing capacity requires purchase of an additional asset block or subscription upgrade at the displayed or agreed fixed price. The block size, price and effective period are specified at purchase. Fees are based on the purchased asset allowance, not actual usage.

2.4 An asset is tested only after the Client explicitly approves it through the platform or another agreed mechanism and confirms the authority required by general clause 5.2.

3. Attack surface discovery

3.1 The Client authorises continuing discovery of internet-facing assets apparently associated with it, using passive and non-intrusive techniques.

3.2 Agentic Security will present newly discovered assets through the platform. The Client may approve or exclude them at any time during the subscription. Assets identified by the Client as not its own will be excluded from further discovery and testing.

3.3 Asset attribution is inferred and may be incorrect. The Client must confirm ownership or permission before approval. Agentic Security does not guarantee discovery of every associated asset.

4. Testing, review and response

4.1 Testing is agent-led, with human oversight and findings review.

4.2 Agentic Security does not guarantee uninterrupted or gap-free discovery or testing. Asset changes, availability, maintenance and third-party restrictions may affect coverage. Critical Findings are handled under general clause 3.6 and, for Partners, Schedule 3 clause 10.2.

4.3 The Client must prioritise remediation, assign responsibility and act on findings. General clause 3.5 governs findings review and triage.

4.4 Agentic Security will provide reports in accordance with the agreed reporting arrangements.

5. Subscription term, renewal and fees

5.1 AEV subscriptions run for 12 months and are payable annually in advance. They renew for successive 12-month terms unless either party gives notice of non-renewal at least 60 days before expiry. Agentic Security will give a renewal reminder and identify the non-renewal deadline at least 90 days before expiry. Partner payment arrangements are governed by Schedule 3 clause 14.

5.2 Renewal price changes require at least 60 days' notice before renewal. The Client may reject the change by giving non-renewal notice within 21 days after receiving it, even if the ordinary deadline has passed. Updated terms apply under general clause 1.7.

5.3 The Client may pause and resume testing during the subscription term. The original expiry date and committed fees continue to apply, and unused time and capacity expire at the end of the term.

5.4 Annual invoices are due under general clause 7.2. Agentic Security may make initial activation conditional on payment. Purchased capacity increases under clause 2.3 are payable in advance for the agreed period within the subscription term, unless an extension is expressly agreed.

6. Suspension, termination and reports

6.1 General suspension and termination provisions apply. During suspension, the original term and committed fees continue, subject to non-excludable rights and clause 6.4.

6.2 On expiry or termination, testing and subscription access end. Agentic Security will provide completed reports under general clause 9.4.

6.3 Copies of reports will be available on request for 30 days after expiry or termination.

6.4 Fees are non-refundable except where required by Law or where the Client terminates for Agentic Security's material breach under general clause 9.1, in which case unused prepaid fees will be refunded pro rata. Schedule 3 governs Partner refunds.

Schedule 3: Partner Terms

1. Application and designation

1.1 This Schedule applies to Partners using either Penetration Testing Services or AEV Subscription Services. It supplements the relevant service Schedule and the general terms, with precedence governed by general clauses 1.4 and 1.6.

1.2 A Client is a Partner only when Agentic Security designates it as one and provisions its separate Partner Account. The Partner uses that account to test End Client Systems in its own capacity as a service provider.

1.3 The Partner contracts as principal, not as agent for an End Client. An End Client is not a party to an Agreement and acquires no contractual rights against Agentic Security under it.

2. Condition of use

2.1 The Partner may submit, confirm or enable a target, or authorise discovery for an End Client, only while it holds sufficient current End Client Authorisation.

2.2 Each such submission, confirmation or enabling is a representation and warranty of that authority. Use without it breaches this Schedule; testing or discovery that follows is Unauthorised Testing.

3. Application to End Client Systems

3.1 Each Client obligation, warranty, consent, acknowledgement and indemnity concerning targets, data or Systems applies to the Partner in respect of its End Clients. References to the Client's Systems, data, customers, Personnel or environment include the corresponding End Client matters.

3.2 This includes scope and authorisation under general clauses 2, 4 and 5, privacy permissions under general clause 11.2, information accuracy under general clause 15.5 and indemnities under general clause 16.6; Schedule 1 readiness duties where penetration testing is purchased; and Schedule 2 discovery and approval duties where AEV is purchased.

4. End Client Authorisation

4.1 End Client Authorisation is current, legally effective permission, recorded in writing or electronically, from a person entitled to bind the End Client and any other owner or operator whose permission is required. It must identify the authorised targets or selection method, cover the testing and discovery methods and period, permit delivery through the Partner's platforms and providers including Agentic Security, and satisfy general clause 5.2.

4.2 The Partner obtains, maintains and records that permission and ensures it remains sufficient. Agentic Security does not undertake to verify it; general clause 5.4 applies.

4.3 If permission expires, is withdrawn or becomes doubtful or insufficient, the Partner must immediately disable affected targets, stop affected testing and notify Agentic Security.

5. Authorisation Attestation

5.1 By accepting these terms and submitting, confirming or enabling a target through the Partner Account, the Partner gives an Authorisation Attestation that it holds the permission required by clause 4 for that target and activity.

5.2 Each attestation applies to the submitted, confirmed or enabled target while its underlying permission remains valid. Any validity date entered in the platform must fall within that permission's term.

5.3 The Partner is accountable for every attestation and action through its Partner Account as if made by the Partner itself.

6. Partner accountability

6.1 The Partner is responsible for scope and authority, its End Client contracts and representations, review and triage of findings, publication and escalation to End Clients, and its users' conduct. It is also responsible for any required End Client, regulatory or other incident notifications.

6.2 The Partner is the sole contractual point of service delivery and communication with its End Clients, subject to obligations imposed by Law.

7. Unauthorised Testing

7.1 Unauthorised Testing means testing or discovery through the Partner Account without sufficient current End Client Authorisation. It includes out-of-scope activity, activity after permission expires or is withdrawn, and activity affecting a third party whose required permission was not obtained. It applies whether initiated by the Partner, an account user or automated systems acting on the Partner's submission or enabled settings.

7.2 If Unauthorised Testing occurs, or the Partner fails to provide authority evidence under clause 13.1, Agentic Security may immediately terminate all Partner Agreements and close the Partner Account by notice. No contractual breach-remedy period applies to that action, subject to non-excludable rights.

7.3 Agentic Security may immediately suspend the account or affected testing without prior notice while investigating reasonably suspected Unauthorised Testing. General clause 5.7 also applies.

7.4 On termination under clause 7.2, paid fees and purchased credits are not refunded, credited or carried forward, except to the extent required by Law. This overrides ordinary contractual refund provisions, including clause 14.2 of this Schedule. Subject to general clauses 5.7, 15.6 and 16.7, Agentic Security is not liable for Loss arising from suspension under clause 7.3 or 13.2 or termination under clause 7.2.

7.5 These remedies do not limit other rights, including clause 8.

8. Partner liability

8.1 The Partner indemnifies Agentic Security and its Personnel against Loss, including indirect and consequential Loss, arising from Unauthorised Testing, breach of this Schedule, or third-party claims connected with Partner testing, discovery or reports, except to the extent caused by Agentic Security's Gross Negligence, fraud or wilful misconduct.

8.2 To the extent permitted by Law, Partner liability under this clause and for Unauthorised Testing or breach of this Schedule is not capped

or excluded by general clause 16. Its consequential-loss exclusion and contractual claim deadline do not apply to that liability.

8.3 For the purposes of clause 8.1 and general clause 16.7, automated execution of a Partner-submitted or enabled target is not, merely because Agentic Security's systems execute it, an act or omission by Agentic Security contributing to Loss. This does not excuse Agentic Security's separate acts or omissions.

8.4 These duties supplement general clauses 5.6 and 16.6 without double recovery and do not exclude rights required by Law.

9. End Client relationships

9.1 The Partner must not bind Agentic Security, make commitments on its behalf or imply that an End Client has a contract with it.

9.2 Agentic Security may refer an End Client enquiry to the Partner.

10. Findings, reports and branding

10.1 Agentic Security makes findings and report content available in the Partner Account. The Partner reviews, validates and triages findings and publishes reports, and is responsible for the accuracy, completeness and presentation of what it publishes.

10.2 For Partner Engagements, the Partner alone is responsible for reviewing findings, correcting reports and notifying End Clients, including of Critical Findings, in place of the direct-client arrangements in general clauses 3.5 and 3.6. Agentic Security will make Critical Findings available to the Partner, including during suspension. The Partner must monitor and escalate them.

10.3 The Partner is responsible for its review decisions, edits, severity changes, representations and publication. Agentic Security remains responsible for its own conduct under general clause 19.5.

10.4 The Partner must publish reports under its own brand and remains responsible for their review and content. Use of Agentic Security's, Cypen's or cypen.ai's names or logos requires Agentic Security's separate prior written approval and compliance with the approved use. Approved branding must identify the Partner as reviewer and publisher; any claim that Agentic Security reviewed or endorsed the report requires express written approval.

10.5 Reports must not be represented as certification or accreditation; general clause 14.5 applies.

10.6 General clause 14.2 applies with the Partner as owner. Despite general clause 14.4, the Partner may share reports with the relevant End Client and edit, extract or apply its own branding to them, subject to clause 10.4.

10.7 The Partner must initiate retesting through the Partner Account and pay the agreed retesting fee.

11. Partner Account

11.1 General clause 18 governs Partner platform access for either service.

11.2 The Partner must not resell or sublicense the platform or give others access to its Partner Account, except to the extent Agentic Security expressly enables end-client or other access.

12. Data

12.1 End Client data is Client Data and, where confidential, the Partner's Confidential Information for the Agreement. Retained testing material is Engagement Fieldwork under general clause 13.

12.2 Agentic Security will keep each End Client's data logically separate. Reuse of client-specific fieldwork for future Services is limited to Partner Engagements for that same End Client.

12.3 The Partner must obtain all permissions and give notices required for End Client Personal Information and ensure its End Client arrangements permit the processing locations and providers agreed under general clauses 11 and 19 and Schedule 4.

12.4 Copies of reports produced for End Clients will be available to the Partner on request for 30 days after expiry or termination, including under clause 7.2. Agentic Security may preserve fieldwork relevant to suspected Unauthorised Testing as reasonably necessary for investigation or proceedings, subject to applicable Law and continued protection under general clause 13.

13. Evidence and cooperation

13.1 Within 5 Business Days of a written request, the Partner must provide the relevant End Client Authorisation and reasonable supporting evidence. Failure to provide it permits the contractual Unauthorised Testing remedies in clause 7.

13.2 Agentic Security may suspend affected targets, engagements or the account while the request remains unanswered; general clause 5.7 applies.

13.3 The Partner must retain authority, attestation and scope records for at least seven years after the relevant testing and reasonably

cooperate in investigating actual or suspected Unauthorised Testing.

13.4 Despite general confidentiality and fieldwork restrictions, Agentic Security may disclose relevant information to the extent reasonably necessary and lawful to investigate, stop or respond to suspected Unauthorised Testing, including to affected system owners, authorities, insurers and advisers.

14. Fees and credits

14.1 Partner fees, credits, packages, capacity limits and payment schedules are those stated in the Agreement or accepted Partner Account order. Those payment arrangements govern Partner Engagements. AEV access remains for a fixed annual term.

14.2 Paid Partner fees and credits are non-refundable except where required by Law or where the Partner terminates for Agentic Security's material breach, in which case unused fees and credits for unperformed Services are refunded. Clause 7.4 applies to termination for Unauthorised Testing.

15. Publicity

15.1 General clause 14.7 applies to the Partner's name and logo. Agentic Security will not identify an End Client without that End Client's prior consent, except as permitted by clause 13.4 or Law.

Schedule 4: Subprocessors

1. Application and location choices

1.1 Agentic Security may use the providers below for the specified purposes and information categories.

1.2 Agreed Australian-only engagement processing uses the Australian delivery and inference options under general clause 11.5. Other engagements may use the Australian and United States options below. Business administration and development use their listed locations, subject to the Agreement.

1.3 Provider-list changes follow general clauses 1.7 and 11.7 and remain subject to agreed residency, confidentiality and security requirements.

2. Service delivery

The following providers support hosting, testing workloads and workflow execution.

Provider	Purpose and information handled	Storage and processing	Location
DigitalOcean	Application and orchestration infrastructure, PostgreSQL database, storage, Client Data and Engagement Fieldwork	Stores and processes engagement and operational data	Australia
OpenComputer	Agentic sandbox workloads for Australian processing; authorised targets, testing context and fieldwork	Processes and holds workload data	Australia
OpenComputer	Agentic sandbox workloads for United States processing; authorised targets, testing context and fieldwork	Processes and holds workload data	United States
Temporal Cloud	Durable workflow orchestration; workflow state and execution context	Stores and processes workflow information	Australia

3. AI inference

The following providers process model inputs and outputs under general clause 19.3.

Provider	Purpose and information handled	Retention and training requirements	Location
SCX.ai	Model inference for engagements requiring Australian processing; Client Data in model inputs and outputs	Zero retention beyond transient processing; no training on inputs or outputs	Australia

Provider	Purpose and information handled	Retention and training requirements	Location
OpenRouter	Intermediary routing Client Data in model inputs and outputs to downstream model providers for inference	Zero retention beyond transient processing and no training on inputs or outputs, covering OpenRouter and selected downstream providers; routing restricted to United States processing	United States

4. Business operations

The following providers handle business administration within the information limits stated below.

Provider	Purpose and information handled	Location
HubSpot	Customer relationship management; business contact information	Australia
MYOB	Accounting and invoicing; business contact and billing information	Australia
Stripe Australia	Payment processing; billing information. Card details are held exclusively in Stripe's environment	Australia
FYXER	Inbox organisation; administrative email information only, excluding Client attachments and engagement content	Europe
Notion	Internal business operations and documentation; excludes Client Data and Engagement Fieldwork	United States

5. Development

The following providers support software development.

Provider	Purpose and information handled	Location
GitHub	Source-code repositories and development material; excludes Client Data, Engagement Fieldwork and production credentials	United States
OpenAI	Software development assistance; source code and development inputs, separate from service-delivery inference; excludes Client Data, Engagement Fieldwork and production credentials	United States