STANDARD TERMS AND CONDITIONS

ASCOVIA LABS

These Standard Terms and Conditions (the "Terms") apply to business orders for managed IT, cybersecurity, and related services from Ascovia Labs LLC, a limited liability company registered in Texas ("Supplier"). The "Customer" is the organization identified in the applicable Statement of Work. These Terms and the documents incorporated under Section 1 form the parties' Agreement. They become binding when the parties sign a Statement of Work that incorporates them, or when they otherwise expressly agree in writing to be bound.

1. Definitions and interpretation

1.1 The terms below have the following meanings when used in the Agreement, including in a Statement of Work, Schedule, or other incorporated document.

Acceptable Use Policy: The Supplier's policy governing permitted use of the Services, available on the Supplier's website, to the extent incorporated into the Agreement.

Additional Charges: Amounts payable for work or expenses outside the agreed scope or price, when approved or authorized in accordance with Section 9.4.

Affiliate: An entity that directly or indirectly controls, is controlled by, or is under common control with a party. Control is the power to direct the entity's management or policies.

Agreement: These Terms, the applicable signed Statement of Work, signed Change Orders, and any schedules, service terms, or addenda expressly incorporated by reference.

Applicable Data Protection Laws: The privacy, data protection, and data security laws and regulations that apply to the relevant data, processing activities, and role of each party, including any applicable breach notification requirements.

Applicable Laws: The statutes, regulations, binding orders, and other legal requirements that apply to a party's performance or use of the Services under the Agreement.

AscoviaDefence: The Supplier's continuous threat validation offering. The Statement of Work identifies the controls to be assessed, the validation activities and reporting included, and the parties' responsibilities for follow-up.

AscoviaSecure: The Supplier's managed IT offering. It may include user support, cloud and infrastructure operations, endpoint management, and service reporting to the extent specified in the Statement of Work.

Authorized Users: The Customer's personnel and other persons it permits to access or use the Services within the agreed scope.

Backup and Disaster Recovery: Work to make or manage copies of data or configurations and to restore agreed data, systems, or functions after disruption, as specified in the Statement of Work.

Business Day: A weekday other than a federal holiday observed in the United States, unless the Statement of Work specifies a different calendar.

Business Hours: The hours during which the applicable service or support channel is available, as specified in the Statement of Work or incorporated support documentation.

Change Control Procedure: The process under Section 6 for requesting, evaluating, and approving changes to the Agreement or the Services.

Change Order: A written amendment approved by authorized representatives of both parties under Section 6 that records the agreed change and any related effect on scope, Charges, timing, or responsibilities.

Change Request: A written proposal by either party to change the Services or their delivery, submitted under Section 6. It becomes binding only when approved as a Change Order.

Charges: The fees, approved expenses, and other amounts payable for the Services under the Agreement, including authorized Additional Charges.

Cloud Services: Hosted applications, infrastructure, storage, or other remotely delivered computing services supplied, administered, or supported within the agreed scope.

Confidential Information: Nonpublic information disclosed or made accessible by or on behalf of a party in connection with the Agreement that is identified as confidential or that reasonably should be understood to be confidential. Examples include credentials, system configurations, security findings, customer records, pricing, business plans, and technical materials. Section 15 sets out the exclusions and rules for required disclosures.

Connectivity Services: Services for configuring, monitoring, or coordinating network connections and related equipment or third-party connectivity, where included in the Statement of Work.

Continuous Threat Validation: The recurring assessment of agreed security controls and exposure against relevant threats and authorized test scenarios, with findings reported under the Statement of Work and its Rules of Engagement.

Customer: The organization identified as the customer in the applicable Statement of Work.

Customer Equipment: Equipment supplied or made available by the Customer or its representatives for use in connection with the Services.

Customer Materials: Data, credentials, documentation, equipment, access, and other materials made available to the Supplier by or on behalf of the Customer for the Services.

Customer Personal Data: Personal Data the Supplier Processes as a Data Processor on behalf of the Customer in providing the Services.

Cybersecurity Services: The agreed work to assess, monitor, validate, or improve the security of

systems and data, including AscoviaDefence where specified in the Statement of Work.

Data: Information in any form that is supplied, accessed, generated, or handled in connection with the Services. Data can include logs, configuration records, business content, and Personal Data.

Data Controller: The party that, alone or together with others, determines the purposes and means of Processing Personal Data, subject to Applicable Data Protection Laws.

Data Processing Addendum: An agreement between the parties covering the Processing of Personal Data, including the instructions, scope, duration, safeguards, and responsibilities for that Processing.

Data Processor: The party that Processes Personal Data on behalf of and under the instructions of a Data Controller, subject to Applicable Data Protection Laws.

Data Subject: The individual to whom Personal Data relates. Any rights attaching to that status depend on Applicable Data Protection Laws.

Deliverables: Reports, documentation, configurations, or other work products a Statement of Work identifies for delivery to the Customer.

Effective Date: The effective date of the applicable Statement of Work, determined in accordance with Section 2.1.

Endpoint: A device such as a workstation, laptop, mobile device, or server identified within the service scope for management, support, or security coverage.

Equipment: Physical hardware and related components, accessories, or replacements furnished, managed, or used in performing the Services.

Initial Term: The first committed period of a Statement of Work, if any, as specified in that Statement of Work.

Intellectual Property Rights: Rights in inventions, patents, copyright, software, trademarks, service marks, trade secrets, designs, and other protected intellectual property, including applicable registrations, applications, and renewals.

Managed Services: Ongoing support, administration, maintenance, monitoring, or remediation of systems within the scope and allocation of responsibilities in the Statement of Work.

Milestone: An agreed date, event, or point of completion for a phase of the Services or a Deliverable, as identified in the Statement of Work.

Personal Data: Information that identifies or can reasonably be linked to an identifiable individual. Applicable Data Protection Laws govern the scope of the term for the legal obligations they impose.

Processing: Any operation performed on Personal Data, such as collecting, accessing, storing, using, disclosing, transferring, or deleting it. Process and Processes have corresponding meanings.

Professional Services: Project or advisory work, such as planning, implementation, migration, configuration, or training, when specified in the Statement of Work.

Renewal Term: A subsequent service period beginning after the Initial Term or another Renewal Term if the signed Statement of Work provides for renewal under Section 2.2.

Rules of Engagement: The parties' written authorization and limits for security validation or testing. They may identify permitted systems and activities, test windows, restrictions, notification contacts, and stop conditions.

Schedule: An attachment, exhibit, or other document that the parties expressly incorporate into the Agreement.

Security Breach: A Security Incident involving unauthorized access to, acquisition of, or disclosure of data. Applicable law and any Data Processing Addendum determine whether an event constitutes a legally reportable breach.

Security Event: An observable occurrence suggesting a possible compromise, policy violation, or failure of a security control. Further investigation may establish whether it is a Security Incident.

Security Incident: A confirmed event compromising the confidentiality, integrity, or availability of a system or data within the agreed scope.

Security Risk: A circumstance that could harm the confidentiality, integrity, or availability of systems or data. A Security Risk may be identified before any Security Event or Security Incident occurs.

Service Level: A response, availability, or other performance measure expressly agreed in the applicable Statement of Work or incorporated Schedule, together with the conditions and exclusions specified there.

Service Period: The period during which a particular Service is scheduled to be provided under the Statement of Work.

Service Terms: Terms for a specific Service, including any applicable service description, support arrangements, or exclusions, where expressly incorporated into the Agreement.

Services: The work identified in a Statement of Work. It may include AscoviaSecure managed IT services, AscoviaDefence continuous threat validation, implementation, ongoing support, advisory work, or related services.

Software: Programs, applications, agents, tools, or related updates furnished or made available in connection with the Services.

Software License: Permission granted by the Supplier or a Third Party to use specified Software within the limits of the applicable Software License Terms.

Software License Terms: The conditions of an applicable Software License, which may govern authorized users, devices, use, duration, renewal, and restrictions.

Statement of Work (SOW): A written document signed by both parties specifying the Services and related terms for an engagement, as described in Section 5.

Subscription Licensing: The right to use Software or access an online service for an agreed subscription period, subject to the applicable license or subscription terms and the Statement of Work.
Subprocessor: A Third Party engaged to Process Customer Personal Data on behalf of the Supplier in its role as a Data Processor.
Supplier: Ascovia Labs LLC, a limited liability company registered in Texas.
Supplier Equipment: Equipment provided by the Supplier for the Services, subject to the ownership and delivery terms in Section 7 and the applicable Statement of Work.
Supplier Personal Data: Personal Data for which the Supplier acts as Data Controller, including information it uses for its own business administration in connection with the Agreement.
Support Operations Procedure (SOP): Support documentation incorporated into the Agreement that describes how to request, prioritize, escalate, and track support, and any applicable hours or responsibilities.
System: An environment, combination of devices and Software, network, application, or hosted infrastructure identified within the Statement of Work or an approved Change Order.
Terms: These Standard Terms and Conditions of Ascovia Labs LLC.
Third Party: A person or organization other than the Customer or the Supplier.
Third-Party Software: Software supplied or licensed by a Third Party, whether the Customer obtains it directly or through the Supplier.
Transaction Taxes: Sales, use, or similar taxes imposed on a transaction under the Agreement, as addressed in Section 9.2.
Usage-Based Services: Services for which Charges vary with an agreed measure of consumption, such as licensed seats, devices, or cloud resources, where the Statement of Work provides for usage-based billing.
Vendor: A Third Party that supplies products, licenses, infrastructure, or services used in connection with the agreed Services.

1.2 A signed Change Order controls for the subject it changes. A data processing addendum controls for conflicts concerning processing of personal data. A SOW or incorporated schedule controls over these Terms to the extent it expressly identifies an exception or addresses a service-specific matter assigned to it by these Terms. These Terms govern all other conflicts. "Including" introduces examples without limiting the general language.

1.3 Unless the context requires otherwise, the singular includes the plural and the plural includes the singular. References to a law include its amendments and replacements to the extent they apply. References to a document included in the Agreement include any amendments made under the Agreement.

1.4 A requirement for written communication may be satisfied by email where permitted by law and the Agreement. Requirements for approval, signatures, or delivery of formal notices continue to apply.

1.5 Each SOW should identify the version of these Terms and any incorporated documents that apply to the engagement. A reference to a policy or service description on a website identifies that document for review. Changes to the document apply to an existing engagement only as provided in Section 2.3 or agreed through Section 6.

2. Commencement and duration

2.1 Each SOW takes effect on its stated effective date or, if it specifies none, when both parties sign it. The agreed service start date may depend on onboarding, delivery of access, or other dependencies stated in the SOW.

2.2 The SOW establishes its initial term, any minimum commitment, renewal arrangements, and any notice period for nonrenewal. A SOW renews automatically only if its signed terms expressly provide for renewal. Ending one SOW leaves other SOWs in effect unless a signed agreement or applicable right provides otherwise.

2.3 The Supplier may post updated Terms for future engagements. The version incorporated into a signed SOW continues to apply to that SOW unless the parties agree to a change in writing or the SOW specifies an amendment procedure that the Supplier follows. Website descriptions, samples, and proposals become contractual commitments only when expressly incorporated.

2.4 The parties will identify any onboarding prerequisites in the SOW or an agreed implementation plan. These may include access approvals, a current asset inventory, required licenses, validation scope, or coordination with an outgoing provider. The parties will record any rescheduling or change in responsibilities under Section 6 if a prerequisite cannot be met.

2.5 A service description, demonstration, sample report, or proposal may help the Customer evaluate the Services. The parties should identify any specific deliverable, acceptance criterion, or performance commitment from that material that they intend to make part of the Agreement.

3. Supplier responsibilities

3.1 The Supplier will perform the Services with reasonable care and skill and provide the Deliverables in accordance with the applicable SOW. The SOW and incorporated support documentation govern support hours, channels, response targets, exclusions, and any remedies for failing to meet an agreed service level.

3.2 The Supplier may designate a service contact and assign qualified employees or subcontractors. The Supplier remains responsible for its subcontractors' performance under the Agreement, subject to Section 12 and any specific terms for independent third-party services. Each party will identify who may approve changes on its behalf.

3.3 The Supplier will observe reasonable security, safety, and access requirements the Customer communicates in advance where relevant to the work. For validation and testing, the Supplier will follow the written scope and rules of engagement, including authorized systems, time windows, and escalation contacts.

3.4 Managed IT and cybersecurity services reduce risk within their agreed scope. They do not guarantee detection of every threat, continuous availability, or prevention of every Security Incident. The SOW identifies monitoring, response, remediation, and recovery responsibilities. The parties will coordinate when an issue requires action from both of them.

3.5 The applicable SOW identifies the Service Terms, support procedures, and third-party licenses that govern each component of the Services. For example, a SOW may specify separate conditions for vendor software, cloud administration, project work, equipment, or network support. For managed support, the parties may document how requests are submitted, prioritized, and escalated and when support is available.

3.6 For AscoviaDefence, the parties will identify the authorized scope and agree on Rules of Engagement before validation begins. The SOW should identify the reporting and escalation arrangements and allocate responsibility for remediation and any follow-up validation. A test result or finding reflects the systems, controls, and conditions assessed at the time.

3.7 The Supplier will notify the Customer of a change to its designated service contact that materially affects coordination. The service contact may direct work within the agreed scope. Authority to change the Agreement remains with the representatives designated under Sections 3.2 and 6.

4. Customer obligations

4.1 The Customer will cooperate with the Supplier, designate an authorized point of contact, provide timely and materially accurate information, and make personnel, systems, premises, and access reasonably available as required by the SOW. The Customer will promptly notify the Supplier of changes that affect the Services, including migrations, changes to privileges, or unsupported systems.

4.2 The Customer will maintain the rights, consents, notices, and licenses needed for the Supplier to perform the Services. Before testing any asset, including a cloud environment or third-party hosted system, the Customer will obtain required permissions and identify any provider restrictions. Neither party may expand a testing scope without written approval.

4.3 The Customer will protect credentials, restrict access to Authorized Users, and ensure those users comply with applicable laws, license restrictions, and the Supplier's Acceptable Use Policy as incorporated into the Agreement. The Customer will promptly notify the Supplier of suspected compromised access or other conditions affecting service security.

4.4 Unless the SOW assigns those tasks to the Supplier, the Customer remains responsible for securing the systems it operates, maintaining usable backups, and verifying that copies can be restored. The parties will review scheduling and costs under Section 6 if a Customer dependency delays performance or changes the scope of work.

4.5 The Customer will make agreed premises, systems, personnel, and facilities available on time and maintain Customer Equipment in a condition reasonably suitable for its role in the Services. The Customer will disclose material site, safety, and access restrictions before work begins and tell the Supplier promptly about changes to those restrictions.

4.6 The Customer will take reasonable steps to prevent unauthorized access to software, accounts, and equipment used in the Services. It will use these resources within the applicable license and notify the Supplier promptly of suspected misuse. The Customer will comply with applicable law and will not use the Services, or knowingly allow their use, for fraud or other unlawful activity.

4.7 If an act or omission by the Customer or its representatives delays performance, the Supplier will explain the dependency and its expected effect when reasonably practicable. The parties will review any necessary extension, rescheduling, or additional work under the SOW and Section 6. Additional Charges remain subject to Section 9.

4.8 Where the SOW includes backup or recovery, it should identify the systems and data covered and which party handles backup monitoring, restore testing, and recovery requests. Any agreed retention, recovery targets, testing schedule, and exclusions will be stated in the SOW or an incorporated Schedule.

5. Statements of Work

5.1 Each SOW will describe the Services and Deliverables, identify the systems or locations covered, and set out relevant responsibilities, milestones, acceptance criteria, third-party dependencies, and commercial terms. The parties may add SOWs for additional work.

5.2 A SOW forms part of the Agreement when both parties sign it. Terms printed on a purchase order or generated by a procurement portal serve administrative purposes and do not amend the Agreement unless both parties expressly accept the change in writing.

5.3 Where a SOW provides for acceptance, the Customer will review Deliverables against its agreed criteria and give notice of material deficiencies within the stated review period. The Supplier will address substantiated deficiencies as provided in that SOW.

5.4 For additional Services, the Customer may give the Supplier a description of the requested work and the information reasonably needed to assess it. The Supplier may provide a proposal or decline the request. If the parties proceed, they will record the agreed scope and commercial terms in a signed SOW or Change Order before the additional work becomes binding.

5.5 If a SOW uses milestones or acceptance testing, it should identify who is responsible for each dependency, what evidence demonstrates completion, the review period, and any agreed procedure for correction and retesting. Any deemed acceptance or acceptance by use must be expressly agreed in the signed SOW.

6. Change control

6.1 Either party may request a change in writing. The request should describe the proposed work, the reason for the change, and its effect on scope, fees, timing, responsibilities, and service levels, as applicable.

6.2 A change to the agreed scope, fees, or commitments takes effect only once authorized representatives approve a written Change Order. Routine operational changes within scope may be made under the SOW's procedures. Urgent action reasonably necessary to protect systems or comply with law is addressed under Section 10. A party must promptly communicate any emergency action affecting the other party.

6.3 The party receiving a Change Request may ask for the information it reasonably needs to evaluate the proposal. The parties should consider any effect on Deliverables, Charges, timing, acceptance, security scope, and third-party commitments. The Supplier should identify any known vendor limits such as minimum subscription quantities or terms.

6.4 A Change Order will identify the provisions or SOW it amends, its effective date, and any agreed transition arrangements. Each party may decline a Change Request. The current Agreement continues to govern until the parties approve the change under Section 6.2.

6.5 The Supplier may make routine operational adjustments under the SOW without a Change Order where they remain within authorized scope and do not materially reduce service quality or alter Charges or agreed obligations. Changes to authorized security testing require written approval under Section 4.2.

7. Equipment, title, and security interest

7.1 When the Supplier sells, leases, or furnishes equipment, the SOW specifies the delivery arrangements, allocation of risk, and conditions for transfer of title. Equipment and software made available on a loan, lease, or subscription basis remain subject to the applicable ownership and license terms.

7.2 The Customer will use Supplier-owned equipment as agreed, take reasonable care of it, and return it as directed after the relevant Services end. Customer-owned equipment remains the Customer's property.

7.3 The applicable SOW should specify any delivery, installation, inspection, and return arrangements for Equipment, including who is responsible for shipping, risk of loss, and costs. The Customer will promptly report missing or visibly damaged items after receipt and follow any agreed inspection or warranty procedure.

7.4 While Supplier Equipment is in the Customer's custody, the Customer will take reasonable care of it, use it for the agreed purposes, and follow reasonable written instructions for storage, handling, and return. It will not dispose of or transfer Supplier Equipment without the Supplier's written authorization. The SOW governs any agreed insurance or replacement obligations.

7.5 To secure amounts due under an applicable SOW, the Customer grants the Supplier a lien in the form of a security interest in Customer-owned Equipment specifically identified as collateral in that signed SOW and lawfully in the Supplier's possession or control. The security interest applies only to the extent the Customer has rights in that Equipment and applicable law permits it. The Customer retains title, subject to the security interest, and authorizes filings reasonably necessary to perfect the interest in the identified collateral.

7.6 Following an uncured payment default under the SOW, the Supplier may retain or enforce its interest

in the collateral to the extent and in the manner permitted by applicable law, including any required notice and disposition procedures. The Supplier will release its security interest upon satisfaction of the secured obligations and take any steps required by law to record the release.

8. Personnel, transition, and non-solicitation

8.1 Each party remains responsible for hiring, supervision, compensation, and employment obligations for its personnel. The performance or transfer of Services does not itself transfer personnel from one party to the other.

8.2 If an engagement requires personnel transition or cooperation, the applicable duties and timing must be set out in a separate signed agreement or in the SOW, subject to applicable law.

8.3 Each party will identify any personnel, access, training, or handover responsibilities it assumes for a transition. Any engagement that requires hiring, transferring, or retaining another party's personnel will be addressed in a separate signed agreement or an expressly agreed SOW provision, subject to applicable law.

8.4 If the parties determine that a personnel restriction is reasonably necessary to carry out their legitimate collaboration under a SOW, they may identify the covered roles and applicable duration in that signed SOW. During the assignment and for the agreed period afterward, up to 12 months, neither party may knowingly target the other party's covered personnel for recruitment or hire them as a result of that targeted recruitment without the other party's prior written consent. The restriction applies only to personnel materially involved in delivering or receiving the Services under that SOW and only to the extent permitted by applicable law.

8.5 Section 8.4 permits general recruiting that does not target the other party's personnel and hiring based on unsolicited applications or pre-existing recruitment discussions. It does not restrict a worker's right to seek, apply for, or accept work on their own initiative.

9. Charges and payment

9.1 The signed SOW specifies fees, currency, invoicing dates, payment deadlines, and any approved expenses. Where the SOW provides for usage-based charges, the Supplier will invoice those charges using the agreed usage metric and rate.

9.2 The Customer will pay applicable sales, use, and similar transaction taxes unless it provides valid exemption documentation. Each party remains responsible for taxes on its own net income. The invoice will identify applicable taxes where required.

9.3 The Customer will promptly identify disputed invoice items in writing and pay undisputed amounts when due. The parties will work in good faith to resolve the dispute and make any necessary adjustment. Late fees, changes to rates, and billing for third-party commitments apply only as agreed in the SOW and permitted by law.

9.4 Additional or out-of-scope services and expenses require advance written approval, except where the signed SOW expressly authorizes them under an agreed procedure. The Supplier will identify any third-party fees or cancellation commitments for which the Customer is responsible.

9.5 Where the SOW allows usage-based billing, it should identify the measured unit, reporting period, rates, and any included allowance or minimum commitment. If the Customer questions the usage recorded on an invoice, the parties will review the relevant records using the invoice dispute procedure in Section 9.3.

9.6 Before a proposed upgrade, migration, reconnection, or vendor replacement that would create transition fees or overlapping subscriptions, the Supplier will identify the expected charges for the Customer's review. The SOW or an approved Change Order governs any resulting Charges or pass-through costs. Each party remains responsible for amounts it owes directly to its own vendors unless the SOW provides otherwise.

9.7 The Customer should send an invoice dispute to the billing contact identified in the SOW or invoice, describe the disputed items, and provide information reasonably available to support its position. The parties will use any billing review deadlines and procedures agreed in the SOW. Payment of the undisputed portion remains due as provided in Section 9.3.

10. Suspension of Services

10.1 The Supplier may suspend or restrict the affected Services as reasonably necessary in response to a material breach, a security threat, a legal requirement, required maintenance, or an event under Section 22.1. Suspension for nonpayment is subject to the applicable SOW and applicable law. Any action should be limited in scope and duration to what the circumstances reasonably require.

10.2 The Supplier will give advance notice when reasonably practicable and legally permitted. It may act promptly to contain an incident or prevent harm, then notify the Customer as soon as reasonably practicable. The parties will cooperate on restoration once the reason for suspension has been addressed.

10.3 Security grounds for suspension may include compromised credentials, suspected ransomware, abuse of the Services, or an unsupported or

misconfigured system that presents a material risk. The Supplier may isolate the affected component while the parties investigate. When permitted and practicable, the Supplier will describe the affected Services, the reason for the action, and the steps it reasonably requires for safe restoration.

10.4 For planned maintenance that is expected to materially affect the Services, the Supplier will use the notice and maintenance arrangements in the SOW or incorporated support documentation. For an urgent interruption, the Supplier may act under Section 10.2. The parties will follow the SOW for any service credits, billing treatment, or remedies during suspension.

11. Dispute resolution

11.1 The parties will first attempt to resolve a dispute through their designated contacts. Either party may escalate an unresolved matter to representatives with authority to settle it. The parties may agree to mediation in writing.

11.2 This process does not prevent either party from seeking emergency or interim relief, complying with legal obligations, or taking action to preserve a claim before a deadline.

11.3 If the designated contacts cannot resolve the dispute, either party may send a written summary of the issue and requested resolution to the other party. Each party will identify a representative with authority to discuss settlement and make reasonable efforts to arrange a discussion. Any agreed escalation deadline will be set in the SOW.

11.4 If the parties agree to mediate, they will agree on the mediator, procedure, place or remote format, and allocation of costs. Mediation is subject to Section 11.2 and any dispute procedure agreed in the SOW.

12. Third-party providers

12.1 Services may depend on products, licenses, cloud platforms, telecommunications, or other services supplied by third parties. The Customer must comply with terms that apply to its use and that are identified or made available to it. Where the Customer contracts directly with a provider, that contract governs the provider's performance.

12.2 The SOW identifies what the Supplier will manage or support for a third-party product or service. The Supplier remains responsible for its own agreed work, including any escalation or coordination duties. The Supplier cannot control changes, outages, or discontinuation decisions by independent providers. The parties will address any resulting scope changes under Section 6.

12.3 For material third-party dependencies, the SOW should identify whether the Customer contracts directly with the Vendor, the Supplier resells or arranges the product or service, or the Supplier only provides integration or support. When applicable, the parties will identify license restrictions, vendor support channels, and responsibility for renewals or cancellation.

12.4 If the Supplier learns of a third-party change that is reasonably likely to materially affect the agreed Services, it will notify the Customer as soon as reasonably practicable and discuss available options within its role. The parties will document any approved replacement, migration, or resulting change under Section 6.

13. Intellectual property

13.1 Each party retains ownership of intellectual property it owned or developed independently of the Agreement. The Customer retains its rights in Customer Materials and grants the Supplier and its authorized subcontractors a limited right to use those materials as needed to provide the Services.

13.2 The Supplier and its licensors retain their rights in tools, software, methods, templates, and materials used to perform the Services. Unless a SOW provides otherwise, after payment for the relevant Deliverables the Customer may use, copy, and share them internally for its business purposes. This permission does not transfer ownership of Supplier tools or extend to third-party components beyond their license terms.

13.3 Any assignment of ownership, extended license, or permission to distribute Deliverables externally must be stated in the SOW. The Customer represents that it has authority to provide the Customer Materials for the agreed work.

13.4 Where a Deliverable incorporates pre-existing Supplier tools or third-party components, the applicable ownership and license terms for those components continue to govern. The parties should identify any bespoke software, source code, configuration files, or documentation that the Customer expects to receive and specify the corresponding rights and formats in the SOW.

13.5 The Supplier's permission to use Customer Materials is limited to performing its obligations under the Agreement. The Supplier will use reasonable measures to limit access to those who need it for that purpose. Following the end of the Services, the parties will address return and retention under Sections 14, 15, and 21.

14. Data protection and processing

14.1 Each party will comply with privacy and data security laws that apply to its role and the data it handles. Where the Supplier processes personal data on the Customer's behalf, the parties will document the processing, instructions, data types, duration, and responsibilities in the Agreement or an applicable data processing addendum before processing begins.

14.2 When acting as the Customer's processor, the Supplier will follow documented lawful instructions, limit access to personnel subject to confidentiality obligations, and apply safeguards appropriate to the data and risk. The Supplier will use subprocessors in accordance with the Agreement and impose the protections required by applicable law. When the Supplier uses personal information for its own business administration, its obligations follow its role and applicable law.

14.3 The Supplier will notify the Customer without undue delay after becoming aware of a breach affecting personal data it processes on the Customer's behalf, subject to any shorter deadline required by law or agreed in the applicable addendum. The Supplier will reasonably assist with security inquiries, rights requests, assessments, and compliance verification as required by applicable law and the Agreement.

14.4 At the end of processing, the Supplier will return or delete the relevant personal data as instructed, except to the extent retention is required by law. Any permitted retention, including in backups, remains subject to applicable security and confidentiality obligations. The parties will use a separate addendum where their engagement requires additional provisions, such as a business associate agreement or specific transfer protections.

14.5 Where the Customer acts as Data Controller, it will provide lawful instructions and obtain any notices, consents, or other permissions required before making Personal Data available to the Supplier. If the parties identify a material change to the purposes or scope of Processing or their respective roles, they will update the applicable documentation before proceeding where required by law.

14.6 The Supplier will apply technical and organizational safeguards appropriate to the nature of the Customer Personal Data and the risk of unauthorized access, disclosure, loss, or alteration. As appropriate to the engagement, these may include access controls, encryption in transit, logging, documented security procedures, and training for personnel permitted to handle the data. The Data Processing Addendum may specify additional safeguards.

14.7 The applicable Data Processing Addendum should set out any notice or approval process for Subprocessors. Where the Supplier engages a Subprocessor, it will use written terms that impose the data protection obligations required by Applicable Data Protection Laws. The Supplier will address cross-border transfers under the Agreement and applicable legal requirements.

14.8 A notice under Section 14.3 should describe the known nature and scope of the breach, the affected data where known, and steps taken or planned to contain it. The Supplier will provide material updates as reasonably available. Each party will coordinate communications with the other to the extent permitted by law and remains responsible for its own legally required notices.

14.9 The parties will document any agreed data export or deletion procedures, including treatment of backup copies, legally required retention, and any confirmation of deletion. The Data Processing Addendum controls if a requirement under this section differs from an agreed processing obligation.

15. Confidentiality

15.1 Each party will use the other party's confidential information only to perform the Agreement or exercise its rights under it. Each party will protect it with reasonable care and disclose it only to personnel, contractors, or advisers who need it for those purposes and are subject to confidentiality duties.

15.2 Confidential information excludes information that becomes public without a breach, was lawfully known without restriction, is received lawfully from another source, or is independently developed without using the disclosed information. If disclosure is legally required, the receiving party will give prompt notice where permitted and disclose only what is required.

15.3 These obligations continue for as long as the information remains confidential. Either party may seek injunctive relief where available under law.

15.4 A party may disclose Confidential Information to representatives with a need to know for the purposes described in Section 15.1. It will require those representatives to protect the information under confidentiality duties and take reasonable steps to address any unauthorized disclosure of which it becomes aware.

15.5 If a party is legally required to disclose Confidential Information, it will, where lawful and reasonably practicable, give the disclosing party a reasonable opportunity to seek limits or protective treatment. The receiving party will provide reasonable cooperation and limit the disclosure to the information it is legally required to provide.

15.6 At the end of the applicable Services, the parties will return or securely dispose of Confidential Information as required by the Agreement. A party may retain information to the extent required by law or expressly permitted under the Agreement, subject to the continuing protections in this section. Section 14 and any applicable Data Processing Addendum govern Customer Personal Data.

16. Indemnity

16.1 The applicable signed agreement or SOW governs any obligation to defend, indemnify, or hold the other party harmless. Any agreed indemnity should specify the claims it covers, how notice must be given, who controls the defense, and how a settlement may be approved.

16.2 If the parties agree to indemnification in a SOW, the SOW should identify which party bears responsibility for each category of claim, including any intellectual property, third-party licensing, or data protection claims the parties agree to cover. It should also address cooperation, reasonable defense costs, consent to settlement, and how the indemnity interacts with Section 17.

17. Limitation of liability

17.1 Any negotiated liability cap, exclusions of damages, or exceptions to those limits are governed by the applicable signed SOW or other signed agreement that expressly applies to the claim. These Terms establish no fixed monetary cap or claim notice deadline.

17.2 The Agreement does not exclude or limit any liability, right, or remedy to the extent applicable law prohibits that exclusion or limitation.

17.3 If the signed SOW includes limitations, it should identify the claims and Services to which they apply and any treatment agreed for equipment, confidentiality, data protection, or indemnification. Any claim notification period or different treatment for losses during suspension applies only as expressly agreed and to the extent permitted by applicable law.

18. Warranties

18.1 The Supplier will perform the Services with the care and skill stated in Section 3. Additional warranties and remedies apply as stated in the signed SOW. Any third-party warranty will be passed through to the Customer to the extent the vendor permits and as agreed in the SOW.

18.2 **To the extent permitted by law, and except for warranties expressly stated in the Agreement, the Supplier disclaims implied warranties of merchantability, fitness for a particular purpose, and noninfringement. This provision preserves warranties and remedies that applicable law does not allow the parties to waive.**

18.3 Where a SOW includes equipment or other items sourced from a Vendor, the Supplier will identify any relevant Vendor warranty and will reasonably assist with a permitted transfer or warranty claim to the extent agreed. Any responsibility the Supplier separately agrees to assume for installation, support, or replacement remains governed by the SOW.

19. Insurance

19.1 Each party will maintain insurance required by applicable law. Any additional coverage, minimum limits, or evidence of coverage required for the engagement are specified in the signed SOW or another signed agreement.

19.2 Where insurance is specified in the signed SOW, it should identify the relevant coverage, limits, period, and any requirements for certificates or other evidence. The parties will follow the SOW procedure for providing and updating that evidence.

20. Termination

20.1 Either party may terminate the affected SOW for a material breach that cannot be cured or remains uncured after written notice and the applicable cure period. The signed SOW controls the notice and cure period. If it does not specify a cure period, the breaching party will have a reasonable opportunity to cure a breach that is capable of cure.

20.2 Any rights to terminate for nonpayment, convenience, repeated breaches, a third-party dependency, or insolvency are subject to the signed SOW and applicable law. The party ending a SOW will provide written notice in accordance with Section 22.5 or the SOW's notice procedure.

20.3 A termination notice should identify the affected SOW, the basis for termination, and the intended effective date. Where a breach may be cured, the initial notice should describe the breach and the cure required or reasonably expected. The parties will use any agreed escalation and notice procedures before termination where the SOW or applicable law requires them.

20.4 If a third-party service essential to the SOW is discontinued or lawfully withdrawn, the parties will review available replacements, continuity arrangements, and the scope affected. Any right to terminate on that basis, including any obligation to pay transition or vendor charges, is determined under the signed SOW and applicable law.

21. Consequences of termination

21.1 When a SOW ends, the Customer will pay fees for Services rendered and approved expenses, plus any amounts due under Sections 21.6 and 21.7 and any noncancelable commitments expressly agreed in the SOW. The parties will return property, revoke access, and coordinate the return or deletion of data under the applicable SOW and Section 14.

21.2 Any transition assistance, export formats, handover periods, or associated fees will be handled as specified in the SOW or an approved Change Order. Expiration or termination does not affect accrued rights or obligations. Terms intended to continue, including payment obligations, intellectual property, data protection, confidentiality, liability provisions, and dispute provisions, survive as applicable.

21.3 The parties will coordinate the return of equipment and other property, the transfer of agreed records or configurations, and the removal of access that is no longer needed. The parties will confirm who is responsible for revoking credentials and removing Supplier tools or agents from Customer systems, subject to any continued access needed for agreed transition work.

21.4 If transition assistance is agreed, the SOW or approved Change Order should state the handover period, data export format, delivery method, responsibilities, costs, and any vendor dependencies. Each party will identify the materials and information it needs from the other to complete the agreed handover.

21.5 Final invoices, early termination charges, and outstanding third-party commitments are handled under Sections 9, 21.6, and 21.7 and the signed SOW. Ending the Services does not change the parties' obligations for data return, confidentiality, or the resolution of a claim that accrued before the end date.

21.6 If the Customer terminates a fixed term SOW for convenience before its committed end date, or the Supplier terminates it under Section 20.1 for the Customer's material breach, an early termination charge becomes due without a separate election by the Supplier. The charge starts with the remaining fixed and minimum committed Charges through the end of the current term. The Supplier will deduct amounts already paid or separately invoiced for that period, costs it reasonably expects to avoid, and net amounts it reasonably expects to recover by redeploying capacity committed to that SOW. The charge excludes uncommitted usage and unexercised renewal periods.

21.7 The Supplier will itemize the early termination charge and the credits in its final invoice. The charge applies subject to applicable law and any different calculation or exception expressly stated in the signed SOW. No charge under Section 21.6 is due when the Customer terminates for the Supplier's material breach or properly exercises an agreed or legally protected right to terminate without charge. The Supplier may recover the same amount only once.

21.8 If the Customer fails to return Supplier Equipment when due, the Supplier may require the Customer to make it available for collection. After reasonable written notice, the Customer will arrange lawful access to the relevant premises during normal business hours so the Supplier may enter and recover its identified Equipment. The Supplier will follow reasonable site security and safety requirements and will limit its entry to the agreed areas and purpose. If access is refused or unavailable, the Supplier may seek lawful recovery through the courts. This provision permits no forced entry, breach of the peace, or access to Customer systems or data.

21.9 The Customer will take reasonable care of Supplier Equipment until its return or lawful collection. The parties will coordinate removal to avoid unnecessary disruption and to protect Customer data, including any agreed data return or deletion steps under Section 14.

22. General provisions

22.1 Neither party is responsible for delay to the extent caused by an event beyond its reasonable control, if it promptly notifies the other party and takes reasonable steps to mitigate the impact. This does not excuse payment for Services already provided. If the disruption continues, the parties will follow the applicable SOW's termination or continuity provisions.

22.2 Neither party may assign the Agreement without the other's prior written consent except as expressly provided in the SOW or applicable law. Each party acts as an independent contractor. The Agreement creates no agency, partnership, joint venture, or third-party beneficiary rights except as expressly agreed.

22.3 The Agreement states the parties' entire agreement for its subject matter. Changes must follow Sections 2 and 6. A waiver applies only to the specific matter waived and must be made in writing by the party granting it.

22.4 If a provision is found unenforceable, the rest of the Agreement remains effective to the extent permitted by law. Rights and remedies under the Agreement are cumulative except where the Agreement expressly provides otherwise.

22.5 Send formal notices in writing to the notice address or contact in the SOW, using any method the SOW requires. If no method is specified, use confirmed email delivery, tracked mail or courier, or hand

delivery with a receipt. A notice is effective on receipt unless the SOW provides otherwise. This section does not govern service of legal process.

22.6 An event beyond reasonable control may include a natural disaster, government action, or a widespread disruption to utilities or communications where the event could not reasonably have been prevented or overcome by the affected party. The party invoking Section 22.1 will identify the obligations affected, give reasonably available updates, and resume performance as soon as reasonably practicable.

22.7 Each party will keep its designated operational and notice contacts current. A party may update its notice details by providing written notice under Section 22.5. The parties may use separate contacts or channels for support, billing, and security communications as identified in the SOW.

22.8 A delay in enforcing a right does not by itself waive that right. If a provision may be narrowed to give it lawful effect, it applies to the extent permitted by law. Any remaining unenforceable portion is severed under Section 22.4.

23. Counterparts and electronic signatures

23.1 The parties may sign the Agreement in counterparts, which together form one agreement. The parties agree to transact electronically and may use electronic signatures or exchange signed copies to the extent permitted by applicable law.

23.2 Each signed counterpart is treated as an original. A signed copy may be exchanged electronically in a format the recipient can retain. The parties may use an agreed electronic signature service or exchange a scanned copy of a manually signed document, subject to applicable law.

24. Governing law

24.1 Texas law governs the Agreement and disputes arising from it without regard to conflict-of-laws rules, subject to controlling federal law and any rights that applicable law makes mandatory.

25. Jurisdiction

25.1 Unless a signed agreement provides a different dispute forum or applicable law requires one, the parties agree to the exclusive jurisdiction of the state courts of competent jurisdiction in Travis County, Texas, or the United States District Court for the Western District of Texas, Austin Division, if it has jurisdiction.