

ACCUSIGHTS LLC · PROTECT AND VCISO SERVICES

AccuSights Protect Services Agreement

The agreement between a Customer and AccuSights LLC for Protect (24x7 SOC / managed detection and response) and vCISO services. Read with Exhibit A (Service Description and SLA Schedule), Exhibit B (vCISO Service Schedule) and Exhibit C (Shared Responsibility Matrix).

VERSION

**Version 2026.10 · Effective
November 1, 2026**

© 2026 AccuSights LLC. All rights reserved.

ISSUED BY

AccuSights LLC

AccuSights LLC, an Illinois limited liability company and wholly owned subsidiary of AccuSights, Inc.
2058 N. Western Ave, Chicago, IL 60647

NOTICES

support@accusights.com
subject "ATTN: Legal Notice"
Security Through Compliance

Plain-language summary (for convenience only — not part of the Agreement)

- **Who you are contracting with.** AccuSights LLC, an Illinois company, delivers Protect (24x7 SOC / managed detection and response) and vCISO services. Its parent, AccuSights, Inc., is not a party to this Agreement and is not liable under it, even though Inc. may send you invoices on the LLC's behalf.
- **What Protect is.** Monitoring, detection and response on the assets you enroll, delivered through agents, log sources and cloud integrations, at the tier (Protect Essentials, Protect Advanced or Protect Complete) and Response Mode you select in your Order Form. Every tier is monitored 24x7x365 with a human analyst acknowledging Severity-1 incidents within 15 minutes and triaging them within 60 minutes. Coverage starts on the Monitoring Start Date, after your agents are deployed and a baseline is set.
- **Not a SIEM.** Protect keeps a working copy of your security telemetry for 90 days to detect and respond to threats, then deletes it. It is not a log-management or records-retention service and is not your system of record; you keep your own logs for as long as CMMC, HIPAA, PCI DSS, your insurer or a litigation hold requires.
- **What Protect is not.** It is not insurance, not a guarantee that every attack will be detected or stopped, and not a substitute for your own patching, backups, MFA and good judgment.
- **Three Response Modes.** *Notify* (we alert, you act), *Collaborate* (we recommend, you execute), *Authorize* (you pre-authorize us to isolate hosts, disable accounts and block indicators on designated assets under approved playbooks). You choose one in the Order Form.
- **Your obligations matter.** Agents on 100% of in-scope endpoints, MFA on admin accounts, critical patches within 30 days, offline or immutable backups, 24x7 escalation contacts, and at least \$1,000,000 of cyber insurance. If a loss traces back to something on your side of the shared-responsibility line (a "Customer-Responsible Event"), AccuSights is not liable for it.
- **SLA credits are the only remedy for SLA misses.** If we miss a Severity-1 acknowledgment target, you get a 5% credit per miss, up to 25% of that month's fee. Credits are your sole and exclusive remedy for service-level failures.
- **Liability is capped.** AccuSights' total liability is limited to the greater of the fees paid for Protect in the prior 12 months and \$1,000. Ransom payments, breach-notification costs, fines, forensics beyond the included scope, business interruption and similar losses are excluded, however they are characterized. You will be asked to acknowledge this separately when you sign.
- **vCISO is advice.** Our vCISO is a fractional advisor, not your officer, employee, fiduciary, HIPAA Security Official, CMMC Affirming Official or DPO. Your management makes the decisions and signs the attestations.

This AccuSights Protect Services Agreement (this "**Agreement**") is entered into as of the Effective Date stated in the first Order Form executed under it, between **AccuSights LLC**, an Illinois limited liability company with its principal office at 2058 N. Western Ave, Chicago, IL 60647 ("**AccuSights**"), and the customer identified in that Order Form ("**Customer**"). AccuSights and Customer are each a "**Party**" and together the "**Parties**." AccuSights Technology Consultants LLC (Dubai, UAE), doing business as AccuSights UAE, which operates accusights.ae, is a separate legal entity; it is not a party to this Agreement, has no obligations under it, and neither AccuSights LLC nor AccuSights, Inc. is liable for its acts or omissions.

1. Parties; Relationship to AccuSights, Inc.

1.1 Contracting entity. AccuSights LLC is a wholly owned subsidiary of AccuSights, Inc., a Delaware corporation. AccuSights LLC is the sole provider of, and the sole contracting party for, the Protect Services and vCISO Services described in this Agreement.

1.2 AccuSights, Inc. is not a party. AccuSights, Inc. is not a party to this Agreement, makes no representation, warranty or promise under it, and has no obligation or liability to Customer arising out of or relating to this Agreement, the Protect Services or the vCISO Services. Customer's remedies for anything arising under this Agreement lie solely against AccuSights LLC. Nothing in this Agreement creates any cross-default, cross-guarantee or joint liability between AccuSights LLC and AccuSights, Inc., and no breach of any agreement between Customer and AccuSights, Inc. (including the AccuSights Terms of Service) is a breach of this Agreement, or vice versa.

1.3 Billing and collection agent. AccuSights, Inc. may act as billing and collection agent for AccuSights LLC. Invoices for Fees under this Agreement may be issued by AccuSights, Inc. "on behalf of AccuSights LLC," and payment to AccuSights, Inc. in that capacity discharges Customer's payment obligation to AccuSights LLC to the extent of the amount paid. Acting as billing agent does not make AccuSights, Inc. a party to, or liable under, this Agreement.

1.4 Relationship to other AccuSights agreements. Customer's use of the AccuSights platform, portal and any Assess, Comply or other services of AccuSights, Inc. is governed by the AccuSights Terms of Service and Customer's agreements with AccuSights, Inc. This Agreement governs only the Protect Services and vCISO Services. The Data Processing Addendum, Acceptable Use Policy and Privacy Policy published at accusights.com/legal (the "**Policies**") are incorporated into this Agreement by reference as they apply to the Protect Services and vCISO Services. The AccuSights Terms of Service are not incorporated into this Agreement as a contracting instrument.

2. Definitions

Capitalized terms have the meanings below or where first defined in this Agreement.

TERM	MEANING
"Agent"	means the software sensor, connector, collector or integration that AccuSights or its licensors provide for installation on, or connection to, In-Scope Assets to collect Telemetry and, where authorized, execute Response Actions.
"Authorized Contacts"	means the individuals Customer designates in the Escalation Matrix (Exhibit A) as authorized to receive notices of Security Events, approve or decline Response Actions, and give instructions on Customer's behalf.
"Customer Data"	means data, content and information that Customer or its Users provide to AccuSights, together with Telemetry collected from In-Scope Assets, excluding Service Data.
"Customer-Responsible Event"	has the meaning in Section 13.4.
"Customer's MSP"	means any managed service provider, IT provider or other third party that Customer engages to administer any part of its environment, whether or not that provider purchased Protect on Customer's behalf.
"Escalation Matrix"	means the list of Authorized Contacts, their roles, contact methods and hours of availability that Customer maintains in the Portal in the form set out in Exhibit A.
"Fees"	means the amounts payable for the Protect Services and vCISO Services stated in an Order Form.
"In-Scope Assets"	means the endpoints, servers, identities, mailboxes, cloud tenants, network devices, web properties and other systems that Customer enrolls for monitoring and that are recorded in the asset inventory in the Portal. An asset that is not enrolled and recorded is not an In-Scope Asset, regardless of whether Customer owns or intended to enroll it.
"MDR" or "Managed Detection and Response"	means the detection, investigation and response components of the Protect Services described in Exhibit A.

TERM	MEANING
"Monitoring Start Date"	means the date on which AccuSights confirms in writing (which may be by notice in the Portal) that the onboarding prerequisites in Section 5.2 have been met and monitoring under the SLA has begun.
"Order Form"	means an ordering document, executed by both Parties by in-site electronic signature or otherwise in writing, that identifies the Protect tier, user count, Response Mode, vCISO package (if any), Fees, Term and any negotiated variations, and that references this Agreement.
"Playbook"	means a documented set of pre-approved Response Actions, conditions and limits for a given class of Security Event, as maintained in the Portal and approved by Customer's Authorized Contacts.
"Portal"	means the AccuSights web console through which Customer views alerts, cases, reports, the asset inventory, the Escalation Matrix, Playbooks, the Risk Acceptance log and evidence.
"Protect Services"	means the SOC Services, MDR and the other monitoring, detection, response and included components described in Exhibit A, at the tier stated in the Order Form.
"Response Action"	means an action taken on an In-Scope Asset in response to a Security Event, including isolating or quarantining a host, disabling or resetting an account or session, revoking tokens, blocking an indicator (IP address, domain, hash or process), terminating a process, or removing a malicious rule or persistence mechanism.
"Response Mode"	means the level of response authority Customer grants AccuSights under Section 6: Notify, Collaborate or Authorize.
"Security Breach"	means a confirmed unauthorized access to or acquisition of unencrypted Customer Data while in AccuSights' possession or control, caused by AccuSights' breach of its security obligations under this Agreement or the DPA. A Security Breach does not include a Security Event or Security Incident on Customer's own systems or In-Scope Assets, which the Protect Services are engaged to monitor.
"Security Event"	means an observable occurrence in Telemetry that AccuSights' detection logic or analysts flag as potentially malicious or anomalous.
"Security Incident"	means a Security Event that AccuSights, after triage, classifies as a confirmed or probable compromise of an In-Scope Asset, at a Severity level defined in Exhibit A.
"Service Credit"	means the credit against Fees described in Section 8 and Exhibit A.

TERM	MEANING
"Service Data"	means data generated by AccuSights' operation of the Protect Services that does not identify Customer or any individual, including detection logic, indicators of compromise, threat intelligence, performance metrics and de-identified aggregate statistics.
"Service Description"	means the description of the Protect tiers, components, Severity definitions, coverage and inclusions in Exhibit A, as updated under Section 22.2.
"SLA"	means the service-level targets in Exhibit A.
"SOC Services"	means the security operations center functions of the Protect Services: continuous collection and analysis of Telemetry, alert triage, case management, escalation and reporting.
"Telemetry"	means logs, events, metadata, process and network data, file attributes, identity and authentication signals, configuration data and similar information collected from In-Scope Assets by Agents and integrations, which may incidentally include file names, message headers, user names and other personal information.
"Term"	has the meaning in Section 15.
"Users"	means the individuals whose seats are counted for per-user pricing under the Order Form, and any other Customer personnel who access the Portal.
"vCISO Services"	means the fractional advisory services described in Section 9 and Exhibit B, at the package stated in the Order Form.

3. Ordering; Cap Acknowledgment

3.1 Order Forms. The Protect Services and vCISO Services are ordered only through an Order Form executed under this Agreement. Each Order Form incorporates this Agreement and its Exhibits. If an Order Form expressly and specifically varies a provision of this Agreement, the Order Form controls for that Order Form only; otherwise this Agreement controls. Purchase orders and other Customer forms are for administrative convenience only and their terms have no effect.

3.2 Separate cap acknowledgment. As a condition of executing the first Order Form, Customer's signatory must separately and affirmatively acknowledge the Limitation of Liability in Section 13, by checking the dedicated acknowledgment box or initialing the Limitation of Liability Acknowledgment at the end of this Agreement. This acknowledgment is a distinct act from signing the Agreement, and Customer confirms that it has been given the opportunity to read Section 13 and to seek independent advice before agreeing to it.

3.3 Authority. Each individual executing an Order Form or acknowledgment represents that he or she has authority to bind the Party for which he or she signs.

3.4 Orders through a Customer's MSP or partner. Where Customer's MSP or an AccuSights Empower partner places the order for Customer's benefit, this Agreement must be accepted either by Customer (the end client) directly or by the MSP acting under written authority from Customer to bind it, and in either case Customer is the party bound by this Agreement. The MSP may invoice Customer for the Protect Services at wholesale or other pricing agreed between the MSP and Customer and remains responsible for collection from Customer under that arrangement, and AccuSights may accept payment from the MSP on Customer's behalf. Customer's obligations in Section 7 apply to Customer and to Customer's MSP acting on its behalf, and neither the MSP nor the partner has any authority to vary this Agreement or make commitments on AccuSights' behalf.

4. Services Generally

4.1 Provision of Services. Subject to this Agreement, AccuSights will provide the Protect Services and any ordered vCISO Services during the Term in a professional and workmanlike manner consistent with generally accepted industry standards for managed security service providers of similar size and scope.

4.2 Nature of the Services. The Protect Services are monitoring, detection and response services. They reduce, but cannot eliminate, the risk of a security incident. AccuSights is not an insurer, guarantor or underwriter of Customer's security, and the Fees are priced on that basis. Customer's own controls, personnel, backups, insurance and decisions remain the primary determinants of Customer's security outcome.

4.3 Included components. Each tier includes the components listed for it in Exhibit A. Components marked as add-ons in Exhibit A (an incident-response retainer, forensic investigation beyond the eight (8) hours included per incident, and regulatory response support) are priced on the Order Form and are available only if ordered in an Order Form or, where Exhibit A so states, at AccuSights' then-current hourly rates.

4.4 Tools and third-party components. AccuSights delivers the Protect Services using its own platform together with Agents, tooling and threat intelligence licensed from third parties. Customer receives a limited, non-exclusive, non-transferable right to install and use the Agents on In-Scope Assets during the Term solely to receive the Protect Services. Customer will not reverse engineer, copy, resell or use the Agents for any other purpose. Third-party components may be subject to additional license terms that AccuSights will make available on request.

5. Onboarding; Monitoring Start Date; Scope Changes

5.1 Onboarding. Following execution of the Order Form, AccuSights will provide deployment instructions, Agent packages and integration guidance. Customer (or Customer's MSP) is responsible for deploying Agents, granting the integration permissions listed in Exhibit A, providing an accurate asset inventory, completing the Escalation Matrix, approving initial Playbooks and confirming the Response Mode. AccuSights will assist with onboarding during Business Hours as defined in Exhibit A.

5.2 Prerequisites to monitoring. Monitoring under the SLA begins only on the Monitoring Start Date.

AccuSights will declare the Monitoring Start Date when, at minimum: (a) Agents are deployed, reporting and healthy on at least ninety-five percent (95%) of the endpoints and servers recorded in the asset inventory; (b) the identity, email and cloud integrations for Customer's tier are connected and receiving Telemetry; (c) the Escalation Matrix contains at least two Authorized Contacts reachable 24x7; (d) the Response Mode and initial Playbooks are approved in the Portal; and (e) AccuSights has completed a baseline period of not less than seven (7) days to tune detections to Customer's environment. Before the Monitoring Start Date, alerts are best-effort only, no SLA applies and no Service Credits accrue.

5.3 Coverage gaps before full deployment. Customer acknowledges that assets not yet enrolled at the Monitoring Start Date are not In-Scope Assets until enrolled and reporting. Customer must reach one hundred percent (100%) Agent coverage of in-scope endpoints within thirty (30) days after the Monitoring Start Date and maintain it under Section 7.

5.4 Scope changes. Customer may add In-Scope Assets and Users at any time through the Portal; added Users are billed under Section 11.4. Customer must notify AccuSights before materially changing its environment in ways that affect Telemetry (for example, migrating tenants, replacing its identity provider, changing EDR configuration or adding a site). Removing assets from scope is Customer's decision and is logged as a Risk Acceptance under Section 10.

5.5 Customer's MSP. If Customer uses a Customer's MSP, Customer will ensure that the Customer's MSP cooperates with AccuSights, does not disable or interfere with Agents or Telemetry, and performs the responsibilities allocated to it in the Shared Responsibility Matrix (Exhibit C). AccuSights may share Security Event information with Customer's MSP as an Authorized Contact. Customer is responsible for the acts and omissions of Customer's MSP as if they were Customer's own.

6. Response Modes and Response Authorization

6.1 Election. Customer elects one Response Mode in the Order Form, and may change it prospectively by written notice through the Portal by an Authorized Contact with change authority. The elected mode applies to all In-Scope Assets unless a Playbook designates specific assets or asset classes for a different mode.

6.2 Notify. In Notify mode, AccuSights detects, triages and notifies Customer's Authorized Contacts of Security Incidents with recommended actions. AccuSights takes no Response Actions on In-Scope Assets. Customer is solely responsible for executing any response. Automated containment features of the Agents are disabled or set to alert-only in Notify mode, and Customer acknowledges that this materially reduces the speed and effectiveness of the Protect Services.

6.3 Collaborate. In Collaborate mode, AccuSights detects, triages, notifies and recommends specific Response Actions, and executes a Response Action only after an Authorized Contact approves it for that Security Incident (which may be by Portal, email, text or recorded call). If no Authorized Contact responds within the decision window stated in the applicable Playbook, AccuSights will continue to attempt contact but will not act, and the delay is a Customer-Responsible Event.

6.4 Authorize. In Authorize mode, Customer hereby authorizes and directs AccuSights, without further notice or approval, to take Response Actions on In-Scope Assets when AccuSights reasonably believes a Security Incident is in progress or imminent, within the conditions and limits of the Playbooks Customer has approved. Without limiting the foregoing, Customer expressly authorizes AccuSights to: (a) isolate or quarantine hosts and endpoints from the network; (b) disable, lock, reset or force re-authentication of user and service accounts and revoke active sessions and tokens; (c) block indicators of compromise, including IP addresses, domains, URLs, file hashes and processes, at the endpoint, identity, email or network layer where AccuSights has the technical means; (d) terminate processes and remove malicious inbox rules, scheduled tasks, services and other persistence mechanisms; and (e) take other containment actions expressly listed in an approved Playbook. Customer may exclude specific assets (for example, life-safety, clinical, production-control or executive systems) from Authorize mode by designating them in the Playbook, in which case Collaborate mode applies to those assets.

6.5 Customer's representations regarding In-Scope Assets. Customer represents and warrants that it owns, or has all rights and authority necessary to authorize AccuSights to monitor and take Response Actions on, every In-Scope Asset, including assets hosted by third parties, personal devices enrolled under Customer's policies, and assets administered by Customer's MSP; that it has given any notices and obtained any consents required by law or contract for such monitoring and actions; and that it will not enroll any asset it is not authorized to enroll. Customer will not designate as an In-Scope Asset any system whose isolation could endanger human life or safety unless it has first disclosed that fact in writing and the Parties have agreed a Playbook for it.

6.6 Business impact of authorized actions. Customer acknowledges that Response Actions, by their nature, may interrupt business operations, disconnect users, lock accounts, prevent access to data, or affect systems that later prove not to have been compromised. Customer accepts that risk as an inherent part of the Protect Services. AccuSights is not liable for any loss, cost, downtime, data inaccessibility or business impact resulting from Response Actions taken in good faith within the elected Response Mode and applicable Playbooks, including actions taken on a reasonable but mistaken belief that a Security Incident was in progress. This Section does not excuse AccuSights from liability, subject to Section 13, for Response Actions taken outside the elected Response Mode, outside an approved Playbook, or with gross negligence or willful misconduct.

6.7 Restoration. After a Response Action, AccuSights will, on request of an Authorized Contact and once AccuSights reasonably determines the threat is contained, reverse the action (for example, un-isolate a host or re-enable an account) or provide instructions for Customer or Customer's MSP to do so. Restoration of data, rebuilding of systems and recovery from backups are Customer's responsibility unless included in the tier or ordered as an add-on.

6.8 Emergency contact when no mode permits action. If AccuSights observes an active Security Incident that it cannot act on under the elected Response Mode, AccuSights will escalate through the Escalation Matrix and document each attempt. Customer's failure to respond is a Customer-Responsible Event.

7. Customer Obligations

7.1 Security baseline. Throughout the Term, Customer will, directly or through Customer's MSP: (a) maintain Agents deployed, reporting and healthy on one hundred percent (100%) of in-scope endpoints and servers, and enroll every new endpoint within five (5) business days of provisioning; (b) enforce multi-factor authentication on all administrative, privileged, remote-access and email accounts; (c) apply patches for vulnerabilities rated critical (CVSS 9.0 or higher, or designated critical by the vendor) within thirty (30) days of release, and other patches within a reasonable time; (d) maintain backups of business-critical data that are immutable or stored offline or otherwise isolated from production credentials, and test restoration at least quarterly; (e) not disable, uninstall, bypass, tamper with or exclude Agents, EDR, logging or Telemetry sources, and promptly restore any that fail; (f) maintain an accurate and complete asset inventory in the Portal, including cloud tenants, remote and personal devices used for Customer business, and third-party-hosted systems; (g) maintain the Escalation Matrix with at least two Authorized Contacts reachable 24x7 by phone and one alternate channel, and update it within one (1) business day of any change; (h) retire or isolate end-of-life or unsupported operating systems and software, or record a Risk Acceptance for each; and (i) maintain the network segmentation, email security and identity configurations recommended by AccuSights, or record a Risk Acceptance.

7.2 Cyber insurance. Customer will maintain throughout the Term cyber-liability insurance, including first-party breach-response, business-interruption and cyber-extortion coverage, with limits of not less than one million dollars (\$1,000,000) per claim, and will provide a certificate of insurance on request. Customer acknowledges that the Fees are not priced to, and AccuSights does not, assume the risks that such insurance is designed to cover.

7.3 Cooperation and incident reporting. Customer will: (a) respond promptly to AccuSights' requests for information, access and decisions; (b) report to AccuSights immediately, and in any event within twenty-four (24) hours, any suspected security incident, lost or stolen device, credential compromise or unauthorized access that Customer becomes aware of by any means; (c) preserve logs, images and other evidence relevant to a Security Incident and not alter or wipe affected systems before AccuSights has had a reasonable opportunity to collect evidence, unless necessary to prevent imminent harm; and (d) implement, or record a Risk Acceptance for, each remediation recommendation AccuSights issues, within the timeframe stated in the recommendation.

7.4 Lawful use. Customer will use the Protect Services only for its own internal security operations and in compliance with applicable law, the Acceptable Use Policy and this Agreement. Customer will not use the Protect Services to monitor any individual in violation of applicable employment, privacy or wiretap laws, and is solely responsible for any notices to and consents from its personnel required for endpoint, email and identity monitoring.

7.5 Regulated data. The Protect Services are designed to operate on Telemetry and are not designed for Customer to upload or store regulated data with AccuSights. Customer will not (a) grant AccuSights access to Protected Health Information ("PHI") unless the Parties have first executed AccuSights LLC's Business Associate Agreement ("BAA"), or (b) enroll systems that store or process Controlled Unclassified Information ("CUI") or otherwise expose CUI to AccuSights unless a CUI-capable enclave or CUI-scoped Protect offering is expressly ordered in an Order Form.

Absent an executed BAA, AccuSights is not a business associate of Customer; absent a CUI-scoped order, AccuSights does not accept CUI, and Customer is solely responsible for any regulated data it exposes. Telemetry from a healthcare environment will incidentally contain PHI. Accordingly, for Customers that are HIPAA covered entities or business associates, a BAA with AccuSights LLC must be executed before the Monitoring Start Date, and AccuSights will not declare the Monitoring Start Date until it is.

7.6 Users and credentials. Customer is responsible for all activity under its Portal accounts and for keeping credentials confidential. Customer will notify AccuSights immediately of any unauthorized use of the Portal.

7.7 Consequence of non-compliance. A failure to meet any obligation in this Section 7 is a Customer-Responsible Event for any Security Incident or loss to which it contributed, suspends the SLA for affected assets while it continues, and, if not cured within thirty (30) days after notice, is a material breach.

8. Service Levels and Service Credits

8.1 Service levels. From the Monitoring Start Date, AccuSights will meet the service levels in Exhibit A, including: human acknowledgment of a Severity-1 Security Incident within fifteen (15) minutes of detection, 24x7x365, on every tier; human triage of a Severity-1 Security Incident within sixty (60) minutes of detection, 24x7x365, on every tier; and Portal availability of ninety-nine and one-half percent (99.5%) measured monthly, excluding scheduled maintenance.

8.2 Service Credits. If AccuSights fails to meet the Severity-1 acknowledgment service level for a Security Incident in a calendar month, Customer is entitled to a Service Credit equal to five percent (5%) of the monthly Protect Fees for that month for each such missed event, up to a maximum aggregate credit of twenty-five percent (25%) of that month's Protect Fees for all service-level failures of any kind in that month. If Portal availability in a calendar month is below 99.5%, Customer is entitled to a Service Credit of five percent (5%) of that month's Protect Fees, and if below 99.0%, ten percent (10%) of that month's Protect Fees, in each case counting toward the same twenty-five percent (25%) monthly maximum.

8.3 Claiming credits. To receive a Service Credit, Customer must submit a claim through the Portal or by email to support@accusights.com with the subject line "ATTN: SLA Credit Claim" within thirty (30) days after the end of the month in which the failure occurred, identifying the Security Incident or outage. AccuSights will validate the claim against its case records within thirty (30) days and apply valid credits to the next invoice. Credits are not refundable in cash, have no value after termination, and may not be carried past the Term.

8.4 Exclusions. No Service Credit accrues, and no service level is breached, for any period or event: (a) before the Monitoring Start Date; (b) attributable to a Customer-Responsible Event, including Agent coverage below the required level, disabled Telemetry, an out-of-date Escalation Matrix or unreachable Authorized Contacts; (c) during scheduled maintenance notified at least forty-eight (48) hours in advance, or emergency maintenance; (d) caused by a force majeure event under Section 24.6; (e) caused by a third-party platform outage (for example, Microsoft 365, Google Workspace or a cloud provider) that prevents Telemetry from reaching AccuSights; (f) during any suspension under Section 11.6 or 16.4; or (g) where Customer is in breach of its payment obligations.

8.5 Sole and exclusive remedy. THE SERVICE CREDITS IN THIS SECTION 8 AND EXHIBIT A ARE CUSTOMER'S SOLE AND EXCLUSIVE REMEDY, AND ACCUSIGHTS' SOLE LIABILITY, FOR ANY FAILURE TO MEET A SERVICE LEVEL. A service-level failure is not, by itself, a breach of this Agreement, a basis for termination for cause, or a basis for any damages claim. Repeated failures may give rise to a termination right only as stated in Exhibit A.

9. vCISO Services

9.1 Scope. If Customer orders a vCISO package, AccuSights will provide the advisory services, hours and deliverables for that package as described in Exhibit B. Hours are allocated monthly; unused hours do not roll over, and hours beyond the monthly allocation are billed at the hourly overage rate stated in the Order Form, as set out in Exhibit B.

9.2 Advisory only; no officer or employee status. The vCISO Services are advisory. AccuSights and the individuals who perform the vCISO Services are independent contractors. They are not officers, directors, employees, agents or representatives of Customer, hold no corporate office with Customer, have no authority to bind Customer, direct Customer personnel, approve expenditures, or represent Customer to any third party, and do not become such by reason of any title, email signature, organization chart, badge, meeting role or introduction. Any use of the titles "Chief Information Security Officer," "CISO," "vCISO," "fractional CISO" or similar in connection with the vCISO Services is descriptive of the service only and does not create officer, employee or fiduciary status or any authority.

9.3 No statutory or regulatory role. Unless expressly stated in an Order Form, and then only as to a named individual who has separately accepted the role in writing and subject to any additional fees and insurance AccuSights requires, no AccuSights personnel will serve as, and Customer will not designate or hold out any AccuSights personnel as: Customer's HIPAA Security Official or Privacy Official (45 C.F.R. § 164.308(a)(2), § 164.530(a)); CMMC Affirming Official or any person who affirms, attests or submits scores or assessments to SPRS or the Department of Defense; SEC disclosure signatory or the person responsible for cybersecurity disclosures; Data Protection Officer under the GDPR, UK GDPR or any similar law; PCI DSS responsible officer; Qualified Individual or CISO under 23 NYCRR Part 500, the FTC Safeguards Rule or any similar regulation; or any other statutory, regulatory, contractual or fiduciary role.

9.4 No authority to attest, sign, file or bind. AccuSights personnel will not sign, certify, attest to, affirm, submit or file any assessment, self-assessment, attestation of compliance, SPRS score, regulatory filing, insurance application, customer security questionnaire, contractual representation or public statement on Customer's behalf. AccuSights may assist Customer in preparing such documents; Customer's own officers are solely responsible for their content, accuracy, submission and any signature.

9.5 Management decides. Customer's board, owners and executive management retain sole responsibility and authority for the adoption, prioritization, funding, staffing and implementation of security and compliance decisions, for accepting or declining risk, and for all statements made to regulators, customers, insurers, auditors, assessors and the public. Deliverables under the vCISO Services are recommendations based on the information Customer provides and conditions at the time of review; they are not decisions, guarantees, certifications, legal advice or audit opinions.

9.6 No fiduciary duty. Nothing in this Agreement creates a fiduciary, trustee, agency or similar relationship. AccuSights owes Customer only the duties expressly stated in this Agreement and the duty to perform the vCISO Services with reasonable care and skill consistent with generally accepted industry practices.

9.7 No third-party reliance. The vCISO Services and deliverables are for Customer's internal use. Customer will not represent to any third party that AccuSights has certified, attested to, audited, assumed responsibility for, or is accountable for Customer's security or compliance posture, and will not provide vCISO deliverables to third parties as evidence of compliance without AccuSights' prior written consent and an appropriate disclaimer. No third party may rely on any vCISO deliverable, and AccuSights has no duty or liability to any third party.

9.8 Conflicts; non-exclusivity. AccuSights provides vCISO Services to many clients, including clients that may compete with Customer, and nothing in this Agreement restricts AccuSights from doing so. AccuSights will not disclose Customer's Confidential Information to any other client and will use reasonable staffing practices to avoid assigning the same individual to direct competitors where Customer identifies them in writing.

9.9 Compliance frameworks. AccuSights is not a C3PAO, CMMC assessor, HIPAA auditor, CPA firm, QSA, ISO certification body or auditor of record, and does not certify, accredit or guarantee Customer's compliance with, or the outcome of any assessment under, any law, regulation or framework. Where the vCISO Services include audit or assessment support, that support is preparatory and advisory, and Customer acknowledges that under 32 C.F.R. § 170.8 and the Cyber AB Code of Professional Conduct, an organization that has consulted for Customer may not participate in Customer's CMMC Level 2 certification assessment for three years.

9.10 Personnel. AccuSights will designate a lead vCISO for Customer and may substitute qualified personnel on reasonable notice. Customer may request replacement of an individual for documented reasonable cause.

10. Customer Risk Acceptance

10.1 Risk Acceptance log. Any recommendation, remediation item, configuration change, Playbook expansion or scope addition that AccuSights issues and that Customer declines, defers beyond the stated timeframe, or does not act on will be recorded in the Portal as a "**Risk Acceptance**," identifying the item, the affected assets, the date and the Authorized Contact who declined or deferred it (or a note that no response was received). Customer may add its own rationale.

10.2 Effect. Customer acknowledges that each Risk Acceptance represents Customer's own business decision to accept the associated risk, that AccuSights has no liability for any Security Incident, loss or SLA failure to the extent attributable to an accepted or unaddressed risk, and that a Security Incident that exploits an accepted or unaddressed risk is a Customer-Responsible Event. The Risk Acceptance log is admissible as the Parties' contemporaneous record of the allocation of responsibility for the items it contains.

10.3 Review. AccuSights will include open Risk Acceptances in the monthly report and, where vCISO Services are ordered, in leadership briefings, so that Customer's management can revisit them.

11. Fees and Payment

11.1 Fees. Customer will pay the Fees stated in each Order Form. Protect Fees are charged per User per month at the tier rate stated in the Order Form (list prices: Protect Essentials \$25, Protect Advanced \$35 and Protect Complete \$50 per User per month), subject to a minimum of ten (10) Users per Order Form. vCISO Fees are charged per package per month. Fees are stated and payable in U.S. dollars.

11.2 Billing frequency. Fees for monthly plans are billed monthly in advance. Fees for annual plans are billed monthly in advance or annually in advance, as the Order Form states. Annual prepayment may carry a discount stated in the Order Form.

11.3 Payment terms. Invoices are due net thirty (30) days from the invoice date, or, where Customer has provided a card or ACH authorization on file, will be charged on the invoice date. Customer authorizes AccuSights (and AccuSights, Inc. as billing agent) to charge the payment method on file for all Fees, true-ups and taxes when due.

11.4 User count and true-up. The User count in the Order Form is a committed minimum for the Term. AccuSights will measure the number of enrolled Users monthly; if the enrolled count exceeds the committed count, AccuSights will invoice the additional Users at the Order Form rate for that month and, for annual plans, prospectively for the remainder of the Term. Reductions below the committed count take effect only at renewal (or, for monthly plans, at the start of the next monthly period on thirty (30) days' notice), and never below ten (10) Users.

11.5 Late payment. Amounts not paid when due accrue interest at one and one-half percent (1.5%) per month, or the maximum rate permitted by law if lower, from the due date until paid. Customer will reimburse AccuSights' reasonable costs of collection, including attorneys' fees, for any amount more than sixty (60) days past due.

11.6 Suspension for non-payment. If any undisputed amount is more than ten (10) days past due, AccuSights may, on written notice, suspend the Protect Services and vCISO Services until paid in full. Customer acknowledges that suspension of monitoring means that In-Scope Assets are not monitored, Response Actions are not taken, and no SLA applies during the suspension, and that Customer bears all risk of any Security Incident occurring or continuing during a suspension for non-payment. Suspension does not relieve Customer of its obligation to pay Fees for the suspended period. AccuSights will reinstate services within two (2) business days after payment; re-onboarding fees may apply if Agents were removed.

11.7 Disputes. Customer must notify AccuSights in writing of any good-faith dispute of an invoice within fifteen (15) days of the invoice date, pay the undisputed portion, and cooperate to resolve the dispute promptly. Amounts not disputed within that period are deemed accepted.

11.8 Taxes. Fees exclude sales, use, VAT, GST, withholding and similar taxes, which Customer will pay or reimburse, other than taxes on AccuSights' net income. If Customer is exempt, it will provide a valid exemption certificate.

11.9 Renewal pricing. AccuSights may increase per-User and package Fees at each renewal by not more than five percent (5%) over the Fees for the immediately preceding term, on at least forty-five (45) days' notice before the renewal date, unless the Order Form states otherwise or the applicable tier's list price has changed more than that and Customer is moving tiers.

11.10 No refunds. Except as expressly stated in this Agreement (including Sections 8, 12.2, 14.1, 16.3, 22.2 and Exhibit A-5) or in the AccuSights Subscription, Renewal, Cancellation and Refund Policy as it applies to the LLC's services, Fees are non-cancellable and non-refundable.

12. Warranties and Disclaimers

12.1 Mutual. Each Party represents and warrants that it is duly organized and in good standing, has authority to enter into this Agreement, and that this Agreement is binding on it.

12.2 Service warranty. AccuSights warrants that the Protect Services and vCISO Services will be performed in a professional and workmanlike manner consistent with generally accepted industry standards. Customer's sole and exclusive remedy, and AccuSights' sole liability, for breach of this warranty is for AccuSights to re-perform the non-conforming service; if AccuSights cannot re-perform within a reasonable time, AccuSights will refund the Fees paid for the non-conforming service for the period of non-conformance. Customer must report a warranty claim within thirty (30) days after the service in question was performed.

12.3 No guarantee of detection, prevention or outcome. CUSTOMER ACKNOWLEDGES AND AGREES THAT:

(a) ACCUSIGHTS DOES NOT GUARANTEE OR WARRANT THAT THE PROTECT SERVICES WILL DETECT, IDENTIFY, PREVENT, CONTAIN, REMEDIATE OR REPORT EVERY THREAT, VULNERABILITY, INTRUSION, MALWARE, MALICIOUS SOFTWARE, MISCONFIGURATION, ANOMALY OR MALICIOUS ACTIVITY AFFECTING CUSTOMER OR ITS IN-SCOPE ASSETS, OR THAT CUSTOMER WILL NOT EXPERIENCE A SECURITY INCIDENT, DATA LOSS, DOWNTIME OR OTHER HARM. THE PROTECT SERVICES REDUCE BUT DO NOT ELIMINATE RISK.

(b) DETECTION DEPENDS ON THE TELEMETRY AVAILABLE TO ACCUSIGHTS, THE COVERAGE AND HEALTH OF AGENTS, THE ACCURACY OF CUSTOMER'S ASSET INVENTORY, THE CAPABILITIES OF THIRD-PARTY TOOLS, AND THE STATE OF THREAT INTELLIGENCE AT THE TIME. ATTACKS THAT DO NOT GENERATE OBSERVABLE TELEMETRY ON IN-SCOPE ASSETS, THAT ORIGINATE ON UNMONITORED SYSTEMS, OR THAT USE NOVEL, ZERO-DAY, LIVING-OFF-THE-LAND, SUPPLY-CHAIN OR NATION-STATE TECHNIQUES NOT DETECTABLE BY COMMERCIALLY REASONABLE MEANS AT THE TIME MAY NOT BE DETECTED, AND ACCUSIGHTS HAS NO LIABILITY FOR ANY FAILURE TO DETECT, PREVENT OR RESPOND TO SUCH AN ATTACK (A "**SOPHISTICATED ATTACK**"). IN THE EVENT OF A DISPUTE AS TO WHETHER AN ATTACK WAS A SOPHISTICATED ATTACK, THE DETERMINATION WILL BE MADE BY REFERENCE TO THE DETECTION CAPABILITIES GENERALLY AVAILABLE TO MANAGED SECURITY PROVIDERS OF SIMILAR SIZE AND SCOPE AT THE TIME OF THE ATTACK, NOT WITH HINDSIGHT.

(c) THE THREAT LANDSCAPE CHANGES CONTINUOUSLY, ADVERSARIES ADAPT TO DEFENSIVE MEASURES, AND NO COMBINATION OF TECHNOLOGY AND HUMAN ANALYSIS CAN ASSURE COMPLETE SECURITY. HUMAN FACTORS WITHIN CUSTOMER'S ORGANIZATION, INCLUDING PHISHING SUSCEPTIBILITY, CREDENTIAL SHARING, POLICY VIOLATIONS, INSIDER MISCONDUCT AND FAILURE TO FOLLOW RECOMMENDATIONS, ARE OUTSIDE ACCUSIGHTS' CONTROL AND ARE A LEADING CAUSE OF SECURITY INCIDENTS.

(d) RESPONSE TIMES AND CONTAINMENT DESCRIPTIONS IN ACCUSIGHTS' MARKETING MATERIALS AND ILLUSTRATIONS ARE TYPICAL EXAMPLES, NOT COMMITMENTS; THE ONLY SERVICE-LEVEL COMMITMENTS ARE THOSE IN EXHIBIT A, AND THE ONLY REMEDY FOR THEM IS SERVICE CREDITS.

(e) ACCUSIGHTS DOES NOT WARRANT THAT THE PROTECT SERVICES OR vCISO SERVICES WILL CAUSE CUSTOMER TO BE COMPLIANT WITH ANY LAW, REGULATION, STANDARD OR FRAMEWORK, TO PASS ANY AUDIT OR ASSESSMENT, TO OBTAIN OR RETAIN INSURANCE, OR TO SATISFY ANY CUSTOMER, PRIME CONTRACTOR OR REGULATOR. EVIDENCE PRODUCED BY THE PROTECT SERVICES IS INFORMATIONAL AND POINT-IN-TIME; THE REGULATOR, ASSESSOR, AUDITOR OR CARRIER MAKES THE FINAL DETERMINATION.

12.4 Disclaimer. EXCEPT AS EXPRESSLY STATED IN SECTIONS 12.1 AND 12.2, THE PROTECT SERVICES, vCISO SERVICES, AGENTS, PORTAL, DELIVERABLES AND ANY THIRD-PARTY COMPONENTS ARE PROVIDED "AS IS" AND "AS AVAILABLE," AND ACCUSIGHTS DISCLAIMS ALL OTHER WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, ACCURACY, AND THOSE ARISING FROM COURSE OF DEALING OR USAGE OF TRADE. ACCUSIGHTS DOES NOT WARRANT THAT THE SERVICES WILL BE UNINTERRUPTED OR ERROR-FREE, THAT AGENTS WILL BE COMPATIBLE WITH ALL CUSTOMER SYSTEMS, OR THAT AUTOMATED DETECTIONS WILL BE FREE OF FALSE POSITIVES OR FALSE NEGATIVES. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY ACCUSIGHTS, ITS PERSONNEL OR PARTNERS CREATES A WARRANTY.

13. Limitation of Liability

13.1 Exclusion of certain damages. TO THE MAXIMUM EXTENT PERMITTED BY LAW, AND EXCEPT FOR THE EXCLUDED CLAIMS, IN NO EVENT WILL EITHER PARTY BE LIABLE TO THE OTHER, UNDER ANY THEORY OF LIABILITY (WHETHER CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, STATUTE OR OTHERWISE) AND HOWEVER CHARACTERIZED, WHETHER AS DIRECT, INDIRECT, CONSEQUENTIAL OR OTHERWISE, FOR ANY: (a) INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, EXEMPLARY OR PUNITIVE DAMAGES; (b) LOST PROFITS, LOST REVENUE, LOST BUSINESS, LOST SAVINGS OR LOSS OF GOODWILL; (c) BUSINESS INTERRUPTION, DOWNTIME OR LOSS OF USE; (d) RANSOM, EXTORTION OR OTHER PAYMENTS DEMANDED BY OR MADE TO ANY THREAT ACTOR, AND ANY COSTS OF NEGOTIATING THEM; (e) COSTS OF BREACH NOTIFICATION, CREDIT OR IDENTITY MONITORING, CALL CENTERS, PUBLIC RELATIONS OR CRISIS COMMUNICATIONS; (f) FORENSIC INVESTIGATION, INCIDENT-RESPONSE, LEGAL, RESTORATION, REBUILD OR RECOVERY COSTS BEYOND THE SCOPE INCLUDED IN CUSTOMER'S TIER; (g) REGULATORY FINES, PENALTIES, ASSESSMENTS OR SETTLEMENTS; (h) AMOUNTS PAID OR PAYABLE TO THIRD PARTIES, INCLUDING CUSTOMER'S OWN CUSTOMERS, PATIENTS, CLIENTS OR EMPLOYEES;

(i) COSTS OF PROCURING SUBSTITUTE SERVICES; OR (j) LOSS, CORRUPTION OR INACCESSIBILITY OF DATA TO THE EXTENT CUSTOMER FAILED TO MAINTAIN BACKUPS MEETING SECTION 7.1(d); IN EACH CASE EVEN IF THE PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND EVEN IF A LIMITED REMEDY FAILS OF ITS ESSENTIAL PURPOSE. THE PARTIES AGREE THAT THE CATEGORIES IN (b) THROUGH (j) ARE EXCLUDED WHETHER OR NOT THEY WOULD OTHERWISE BE CHARACTERIZED AS DIRECT DAMAGES.

13.2 Cap. TO THE MAXIMUM EXTENT PERMITTED BY LAW, AND EXCEPT FOR THE EXCLUDED CLAIMS, THE TOTAL AGGREGATE LIABILITY OF ACCUSIGHTS AND ITS AFFILIATES, LICENSORS, SUBCONTRACTORS AND PERSONNEL, ARISING OUT OF OR RELATING TO THIS AGREEMENT, THE PROTECT SERVICES OR THE vCISO SERVICES, FOR ALL CLAIMS OF ANY KIND IN THE AGGREGATE, WILL NOT EXCEED THE GREATER OF (a) THE FEES PAID OR PAYABLE BY CUSTOMER TO ACCUSIGHTS LLC FOR THE PROTECT SERVICES (OR, FOR CLAIMS ARISING FROM THE vCISO SERVICES, THE vCISO SERVICES) UNDER THIS AGREEMENT IN THE TWELVE (12) MONTHS IMMEDIATELY PRECEDING THE EVENT FIRST GIVING RISE TO THE CLAIM, AND (b) ONE THOUSAND DOLLARS (\$1,000). FEES PAID TO ACCUSIGHTS, INC. FOR ANY OTHER OFFERING ARE NOT INCLUDED IN THE CALCULATION. MULTIPLE CLAIMS DO NOT ENLARGE THE CAP, AND SERVICE CREDITS AND REFUNDS PAID ARE COUNTED AGAINST IT.

13.3 Super-cap by election only. If, and only if, an Order Form expressly states that the "Security Breach Super-Cap" applies, then solely for claims arising from a Security Breach (as defined in Section 2, being AccuSights' own confirmed breach of Customer Data in its possession caused by AccuSights' breach of its security obligations), the cap in Section 13.2(a) is increased to two (2) times the Fees described in Section 13.2(a). The super-cap does not apply to Security Events, Security Incidents or any compromise of Customer's own systems or In-Scope Assets, and does not apply unless elected in a signed Order Form. Absent that election, Section 13.2 applies to all claims.

13.4 Customer-Responsible Events — no liability. Notwithstanding anything else in this Agreement, and before any cap applies, AccuSights has no liability of any kind, and no service level is breached, for any Security Incident, loss, damage, cost or claim to the extent arising from or contributed to by any of the following (each a "**Customer-Responsible Event**"): (a) a recommendation, remediation item or Playbook that Customer declined, deferred, delayed or failed to implement, including any item recorded as a Risk Acceptance or for which no response was received; (b) an alert, notification or escalation that Customer ignored, did not acknowledge or did not act on within the applicable Playbook window; (c) malicious, negligent or unauthorized acts of Customer's own personnel, contractors or Customer's MSP, including insiders; (d) phishing, social engineering, business-email compromise or credential compromise not caused by AccuSights' breach of this Agreement; (e) misconfiguration of Customer's systems, identity provider, cloud tenants, email or network by Customer, Customer's MSP or any other vendor; (f) Agents or Telemetry sources that were disabled, uninstalled, tampered with, misconfigured, not deployed, not reporting or excluded, or any resulting gap in Telemetry; (g) systems, accounts, tenants or locations that were not In-Scope Assets at the time of the event; (h) inaccurate, incomplete or outdated asset inventories, Escalation Matrices, evidence or other information supplied by Customer; (i) end-of-life, unsupported or unpatched software or hardware, or failure to patch within Section 7.1(c); (j) failures, outages, vulnerabilities or breaches of third-party products, platforms or vendors, including cloud providers, software vendors, Customer's MSP and supply-chain compromises; (k) force majeure events; (l) a Sophisticated Attack as described in Section 12.3(b); (m) Customer's failure to maintain backups meeting Section 7.1(d), or the failure of those backups;

(n) Customer's selection of Notify or Collaborate mode where a Response Action available in Authorize mode would have contained the incident; or (o) any other breach of Section 7 by Customer or Customer's MSP.

13.5 Excluded Claims. "Excluded Claims" means: (a) a Party's fraud, willful misconduct (including conduct that would constitute willful and wanton misconduct under Illinois law) or gross negligence; (b) Customer's payment obligations under Section 11; (c) Customer's indemnification obligations under Section 14.2; (d) either Party's infringement or misappropriation of the other Party's intellectual property rights; and (e) AccuSights' indemnification obligations under Section 14.1, provided that AccuSights' aggregate liability under Section 14.1 will not exceed two (2) times the cap in Section 13.2(a). Sections 13.1 and 13.2 do not apply to Excluded Claims.

13.6 Allocation of risk; independent limitations. The Parties agree that the exclusions and limitations in this Section 13 are an essential basis of the bargain, that the Fees would be substantially higher without them, that AccuSights is not an insurer and does not price the Protect Services to bear Customer's first-party incident costs or third-party exposure, and that Customer has the means to insure those risks under Section 7.2. Each limitation in this Section 13 is separate and independent, and applies even if any exclusive remedy in this Agreement fails of its essential purpose. This Section 13 applies to the fullest extent permitted by applicable law and is to be construed, where necessary, so as to be enforceable rather than void.

13.7 Claims against personnel. Customer agrees that it will bring any claim arising out of this Agreement only against AccuSights LLC and not against any individual employee, analyst, engineer, vCISO, officer, member, manager or subcontractor of AccuSights, all of whom are intended third-party beneficiaries of this Section 13.

14. Indemnification

14.1 By AccuSights. AccuSights will defend Customer against any third-party claim alleging that the Portal or the AccuSights-developed components of the Protect Services, as provided by AccuSights and used in accordance with this Agreement, infringe a United States patent, copyright or trademark or misappropriate a trade secret, and will pay damages finally awarded or agreed in settlement. AccuSights has no obligation for claims arising from: third-party components, Agents or tools licensed from others (which are subject to those licensors' terms); Customer Data or Customer's systems; combinations with items not supplied by AccuSights; modifications not made by AccuSights; use after notice to stop; or Customer's breach. If a claim is made or likely, AccuSights may modify or replace the affected component, procure a license, or terminate the affected service and refund prepaid unused Fees for it. This Section 14.1 states AccuSights' entire liability for infringement.

14.2 By Customer. Customer will defend AccuSights, its affiliates (including AccuSights, Inc.), and their members, managers, officers, employees, subcontractors and agents against any third-party claim, including claims by Customer's own customers, patients, clients, employees, regulators, insurers and Customer's MSP, arising out of or relating to: (a) Customer Data or its collection, content or use; (b) Customer's or its Users' or Customer's MSP's violation of law, including employee-monitoring, privacy and wiretap laws, or of the Acceptable Use Policy; (c) In-Scope Assets that Customer was not authorized to enroll or on which it was not authorized to permit monitoring or Response Actions, or any breach of Section 6.5; (d) a Customer-Responsible Event;

(e) Customer's use of any deliverable, evidence or vCISO output in violation of Section 9.7, or any representation Customer makes to a third party about AccuSights' services; or (f) any Security Incident affecting Customer's systems, except to the extent finally determined to have been caused by an Excluded Claim on the part of AccuSights; and will pay damages, fines, costs and attorneys' fees finally awarded or agreed in settlement.

14.3 Procedure. The indemnified Party will give prompt written notice of the claim (delay relieves the indemnifying Party only to the extent prejudiced), give the indemnifying Party sole control of the defense and settlement (except that no settlement may impose liability or admissions on the indemnified Party without its consent, not to be unreasonably withheld), and provide reasonable cooperation at the indemnifying Party's expense. The indemnified Party may participate with its own counsel at its own expense.

15. Term

15.1 Agreement term. This Agreement begins on the Effective Date and continues until all Order Forms have expired or been terminated.

15.2 Order Form term; annual and monthly plans. Each Order Form states whether it is an annual plan or a monthly plan. An annual plan has an initial term of twelve (12) months from the Monitoring Start Date (or, for vCISO-only orders, from the Order Form Effective Date), unless the Order Form states a different initial term (the "**Initial Term**"). A monthly plan runs month to month from the Monitoring Start Date (or, for vCISO-only orders, from the Order Form Effective Date), with each monthly period being its Initial Term or a Renewal Term. Fees for the period between the Order Form Effective Date and the Monitoring Start Date are stated in the Order Form; if the Order Form is silent, onboarding is included and Protect Fees begin on the Monitoring Start Date.

15.3 Renewal. An annual plan automatically renews for successive twelve (12) month terms, and a monthly plan automatically renews for successive one (1) month periods (each a "**Renewal Term**" and, with the Initial Term, the "**Term**"), unless either Party gives written notice of non-renewal at least thirty (30) days before the end of the then-current Term. AccuSights will send a renewal reminder at least forty-five (45) days before each annual renewal date.

16. Termination and Suspension

16.1 For cause. Either Party may terminate this Agreement or the affected Order Form on written notice if the other Party materially breaches this Agreement and fails to cure within thirty (30) days after written notice describing the breach (ten (10) days for non-payment). A service-level failure is not a material breach except as stated in Exhibit A.

16.2 Insolvency. Either Party may terminate immediately on notice if the other Party becomes insolvent, makes an assignment for the benefit of creditors, has a receiver appointed, or becomes the subject of a bankruptcy proceeding not dismissed within sixty (60) days.

16.3 For convenience by Customer. Customer may cancel a monthly plan for convenience on thirty (30) days' written notice, with Fees payable through the end of the notice period.

Customer may terminate an annual plan for convenience on sixty (60) days' written notice, provided that, unless the Order Form states otherwise, Customer pays, on or before the termination date, the Fees for the remainder of the then-current Term at the committed User count, less any discount forfeited under the Order Form.

AccuSights may terminate an Order Form for convenience at the end of the then-current Term by non-renewal under Section 15.3, and otherwise only on ninety (90) days' notice with a pro-rata refund of prepaid unused Fees.

16.4 Suspension for security or misuse. AccuSights may suspend the Protect Services, the Portal or any Agent function immediately on notice if AccuSights reasonably determines that (a) Customer's use threatens the security, integrity or availability of AccuSights' platform or other customers; (b) Customer is in breach of the Acceptable Use Policy or Section 7.4 or 7.5; or (c) suspension is required by law or a governmental order. AccuSights will limit the suspension to what is reasonably necessary and lift it when the cause is resolved. A suspension under this Section is not a breach by AccuSights, and Customer bears the risk of Security Incidents during it.

16.5 Effect of termination. On expiration or termination: (a) all Fees accrued through the termination date, and any amounts under Section 16.3, become immediately due; (b) Customer's right to use the Agents and Portal ends, subject to Section 17; (c) monitoring, Response Actions and the SLA cease at 11:59 p.m. Central Time on the termination date, and Customer is solely responsible for its security from that time; and (d) Sections 1.2, 1.3, 2, 6.6, 7.5, 9.2 through 9.7, 10.2, 11, 12.3, 12.4, 13, 14, 16.5, 17, 18 (including 18.10), 19.5, 21, 23, 24 and any other provision that by its nature should survive, survive.

17. Offboarding; Data Export and Deletion

17.1 Agent removal. Within thirty (30) days after termination, Customer (or Customer's MSP) will uninstall all Agents from its systems and revoke the integration permissions granted to AccuSights. AccuSights will provide uninstall instructions and, on request, remote uninstall commands where the tooling permits. AccuSights may remotely disable Agents that remain installed after that period.

17.2 Data export. For thirty (30) days after termination, Customer may export from the Portal, in a commonly used electronic format, its case records, incident reports, evidence artifacts, monthly reports, Risk Acceptance log and vCISO deliverables. Raw Telemetry is available for export only to the extent it remains within the ninety (90) day retention period in Section 18.3, and Telemetry older than ninety (90) days no longer exists and cannot be exported. AccuSights will provide reasonable assistance with export at its then-current hourly rates.

17.3 Deletion. Beginning sixty (60) days after termination, AccuSights will delete or de-identify Customer Data in its production systems, and will purge Customer Data from backups within ninety (90) days after termination, except (a) Service Data, (b) records AccuSights is required by law, regulation or legal hold to retain, and (c) records of the Parties' contractual relationship (Order Forms, acceptance logs, invoices, correspondence). On request, AccuSights will confirm deletion in writing.

17.4 Transition to a successor provider. On request, and at its then-current hourly rates, AccuSights will provide reasonable transition assistance to Customer's successor provider for up to thirty (30) days after termination, provided all undisputed Fees have been paid.

18. Data, Privacy and Security

18.1 Ownership. As between the Parties, Customer owns Customer Data. Customer grants AccuSights and its subcontractors a non-exclusive, worldwide, royalty-free license during the Term (and thereafter for the purposes in Sections 17 and 18.4) to collect, store, process, analyze, transmit and display Customer Data to provide the Protect Services and vCISO Services, to comply with law, and as otherwise permitted by this Agreement. AccuSights owns the Portal, Agents, detection logic, Playbook templates, reports templates, methodologies and Service Data, and all improvements to them. Deliverables under the vCISO Services are licensed to Customer for its internal use on payment of the applicable Fees; AccuSights retains ownership of its pre-existing materials and templates embodied in them.

18.2 Telemetry and monitoring notice. Customer acknowledges that the Protect Services necessarily involve continuous collection of Telemetry from In-Scope Assets, including devices used by Customer's personnel, and may reveal user activity, file names, message metadata, browsing and login patterns and, incidentally, personal information. Customer is responsible for providing any notices to, and obtaining any consents from, its personnel and other data subjects required by applicable law, and for its own privacy and employee-monitoring policies.

18.3 Retention. AccuSights retains Telemetry and alert data for ninety (90) days from collection on every tier, after which it is deleted on a rolling basis. There is no archival tier and no extended-retention option. Case records, incident reports and evidence artifacts are retained for the Term plus the period in Section 17. Retention of logs and records beyond ninety (90) days is Customer's responsibility under Section 18.10.

18.4 Service Data and threat intelligence. AccuSights may use Telemetry and Security Event information to create and use Service Data, indicators of compromise, detection content and de-identified aggregate statistics for the benefit of all its customers, to improve the Protect Services, and for benchmarking and research, provided that Service Data does not identify Customer or any individual. AccuSights may share indicators of compromise with trusted threat-intelligence communities and vendors in de-identified form.

18.5 DPA; BAA. The AccuSights Data Processing Addendum ("**DPA**") is incorporated into this Agreement and governs personal information in Customer Data, with AccuSights LLC as the processor or service provider. Where Customer is a HIPAA covered entity or business associate and PHI may be present in Telemetry, the Parties will execute AccuSights LLC's BAA before the Monitoring Start Date, and the BAA governs PHI. In the event of conflict regarding personal information or PHI, the BAA controls over the DPA, and the DPA controls over this Agreement.

18.6 AccuSights' security. AccuSights will maintain an information security program with administrative, technical and physical safeguards appropriate to the sensitivity of Telemetry and consistent with recognized industry frameworks, as summarized in the Security and Trust Statement at accusights.com/legal, including encryption of Customer Data in transit and at rest, role-based access, MFA for AccuSights personnel, logging of access to Customer Data, and background checks for personnel with access to Customer environments.

AccuSights will notify Customer without undue delay, and in any event within seventy-two (72) hours, after confirming a Security Breach, and will provide information reasonably required for Customer to meet its own notification obligations.

18.7 Law-enforcement and legal requests. If AccuSights receives a subpoena, warrant, court order or other legal demand for Customer Data, AccuSights will, unless legally prohibited, notify Customer promptly so that Customer may seek a protective order, will disclose only what is legally required, and will cooperate reasonably with Customer at Customer's expense. AccuSights may disclose Customer Data without notice where it reasonably believes disclosure is necessary to prevent imminent harm to persons or to AccuSights' platform, or where notice is prohibited by law.

18.8 AI-assisted analysis. The Protect Services use machine learning and AI models, including third-party models, to triage and analyze Telemetry. AI outputs may be inaccurate and are reviewed by AccuSights personnel before any Response Action is taken or recommendation is issued. Customer Data is not used to train AccuSights' or any third party's foundation models; AccuSights uses AI providers only under enterprise terms that prohibit training on Customer Data and restrict the provider to processing Customer Data solely to provide services to AccuSights.

18.9 Location and subprocessors. Customer Data is hosted in the United States on Microsoft Azure (primary region East US 2) and Amazon Web Services (US regions), using the subprocessors listed at accusights.com/legal/subprocessors. AccuSights will give notice of new subprocessors and an objection right as stated in the DPA.

18.10 Not a SIEM; Secondary Logs. AccuSights Protect ingests copies of security telemetry and event data solely to detect and respond to threats. Those copies are secondary, read-only working data, retained for ninety (90) days and then deleted. AccuSights is not a SIEM, log-management or records-retention service and is not the Customer's system of record. Customer remains solely responsible for retaining its own logs and records for the periods required by CMMC and NIST SP 800-171 (AU family), HIPAA, PCI DSS, its insurer, litigation holds, or any other obligation. AccuSights will provide export assistance for data still within the ninety (90) day window on request at its then-current hourly rate. AccuSights has no liability for the unavailability of Telemetry older than ninety (90) days.

19. Confidentiality

19.1 Definition. "Confidential Information" means non-public information disclosed by a Party (the "Discloser") to the other (the "Recipient") in connection with this Agreement that is marked confidential or that a reasonable person would understand to be confidential, including, for Customer, Customer Data, security architecture, incident details and vulnerabilities, and, for AccuSights, the Portal, detection logic, Playbook templates, pricing, personnel information, security practices and the terms of this Agreement.

19.2 Obligations. The Recipient will use Confidential Information only to perform or receive services under this Agreement, will protect it with at least reasonable care, and will disclose it only to its and its affiliates' employees, contractors, subcontractors, advisors and insurers who need to know it and are bound by obligations at least as protective. The Recipient is responsible for their compliance.

19.3 Exceptions. Confidential Information does not include information that the Recipient can show (a) was publicly available without breach; (b) was known to it before disclosure without restriction; (c) was received from a third party without restriction; or (d) was independently developed without use of the Discloser's Confidential Information.

19.4 Compelled disclosure. The Recipient may disclose Confidential Information to the extent required by law or legal process, after giving the Discloser prompt notice (where permitted) and reasonable cooperation to seek protection.

19.5 Duration; remedies. These obligations continue for five (5) years after termination, and for Customer Data and trade secrets for as long as they remain confidential. Each Party acknowledges that breach may cause irreparable harm for which injunctive relief is appropriate without the need to post bond.

19.6 Incident details. Customer may share Security Incident details with its insurers, counsel, forensic firms and regulators; AccuSights may share them with its insurers, counsel and, in de-identified form, as Service Data.

20. Insurance

20.1 AccuSights. AccuSights maintains technology errors & omissions and cyber liability insurance with carriers rated A- or better; a certificate of insurance is available on request. AccuSights' insurance is for AccuSights' own protection and is not a source of recovery for Customer beyond Section 13.

20.2 Customer. Customer will maintain the cyber-liability insurance required by Section 7.2 and will name no party as additional insured; Customer's insurance is Customer's primary source of recovery for first-party incident costs.

21. Subcontractors and Personnel

21.1 Subcontractors. AccuSights may use vetted subcontractors, including SOC analysts, incident responders, threat-intelligence providers, tooling vendors and cloud infrastructure providers, to perform parts of the Protect Services and vCISO Services. AccuSights will require subcontractors with access to Customer Data to be bound by confidentiality and security obligations consistent with this Agreement, will conduct reasonable due diligence on them, and remains responsible to Customer for their performance as if it were AccuSights' own.

21.2 Non-solicitation of SOC and vCISO staff. During the Term and for twelve (12) months after it ends, Customer will not, directly or through Customer's MSP or any agent, solicit for employment or engagement any AccuSights employee or contractor who performed SOC, incident-response or vCISO services for Customer, without AccuSights' prior written consent. General advertisements not targeted at AccuSights personnel are not solicitation. If Customer breaches this Section, Customer will pay AccuSights, as liquidated damages and not as a penalty, an amount equal to fifty percent (50%) of the individual's annualized compensation at AccuSights, which the Parties agree is a reasonable estimate of AccuSights' recruiting and training cost.

22. Amendments; Changes to Service Description

22.1 Signed writing. This Agreement and each Order Form may be amended only by a written amendment signed (including by in-site electronic signature) by authorized representatives of both Parties. AccuSights will not unilaterally change this Agreement or any Order Form during its Term. Posted changes to the AccuSights Terms of Service do not amend this Agreement.

22.2 Service Description and SLA. AccuSights may update Exhibit A and the Policies from time to time to add features, improve service levels, reflect changes in tooling or threat landscape, or clarify processes, provided that no such update materially degrades the service levels, Service Credits, coverage or included components of Customer's tier during the then-current Term without Customer's written consent. AccuSights will give at least thirty (30) days' notice of updates by email to Customer's Authorized Contacts and in the Portal. If an update to the Policies that applies to the Protect Services materially reduces Customer's rights or increases its obligations, Customer may terminate the affected Order Form by notice before the effective date and receive a pro-rata refund of prepaid unused Fees. Changes to Playbooks require approval by Customer's Authorized Contacts and are not amendments to this Agreement.

23. Governing Law; Dispute Resolution

23.1 Governing law. This Agreement is governed by the laws of the State of Illinois, without regard to its conflict-of-laws rules. The United Nations Convention on Contracts for the International Sale of Goods and the Uniform Computer Information Transactions Act do not apply.

23.2 Venue. Each Party irrevocably submits to the exclusive jurisdiction of the state and federal courts located in Cook County, Illinois, for any dispute arising out of or relating to this Agreement, and waives any objection to venue or inconvenient forum. Either Party may seek injunctive relief in any court of competent jurisdiction to protect its intellectual property or Confidential Information.

23.3 Jury waiver. TO THE FULLEST EXTENT PERMITTED BY LAW, EACH PARTY KNOWINGLY, VOLUNTARILY AND INTENTIONALLY WAIVES ANY RIGHT TO A TRIAL BY JURY IN ANY ACTION ARISING OUT OF OR RELATING TO THIS AGREEMENT.

23.4 No class actions. Each Party will bring claims against the other only in its individual capacity and not as a plaintiff or class member in any purported class, collective, consolidated or representative proceeding.

23.5 Time to bring claims. Except for claims to collect unpaid Fees and Excluded Claims under Section 13.5(a), any claim arising out of or relating to this Agreement must be filed within one (1) year after the claimant knew or reasonably should have known of the facts giving rise to it, or it is permanently barred.

23.6 Escalation before suit. Before filing suit (other than for injunctive relief or collection), a Party will give the other written notice of the dispute, and executives of each Party with settlement authority will confer in good faith, in person or by video, within thirty (30) days. The one-year period in Section 23.5 is tolled during that thirty-day period.

23.7 Attorneys' fees. In any action by AccuSights to collect unpaid Fees, the prevailing party is entitled to its reasonable attorneys' fees and costs. Otherwise each Party bears its own fees.

23.8 Regulatory and legal cooperation. If Customer requires AccuSights' assistance with a regulatory inquiry, audit, insurance claim, litigation or law-enforcement matter relating to a Security Incident (including producing records, preparing declarations, or participating in interviews), AccuSights will provide reasonable assistance at its then-current hourly rates plus expenses, subject to Section 19 and any legal restrictions. Nothing in this Agreement obligates AccuSights or its personnel to provide testimony, expert opinions or certifications beyond what is compelled by law, and any such compelled participation is at Customer's expense to the extent permitted by law.

24. General

24.1 Independent contractors. The Parties are independent contractors. Nothing in this Agreement creates a partnership, joint venture, agency, franchise, employment or fiduciary relationship.

24.2 Assignment. Neither Party may assign this Agreement without the other's prior written consent, not to be unreasonably withheld, except that AccuSights may assign it without consent to an affiliate or to a successor in a merger, acquisition or sale of substantially all of the assets of its Protect business, on notice to Customer. Any other purported assignment is void. This Agreement binds permitted successors and assigns.

24.3 Notices. Notices under this Agreement must be in writing and sent (a) to AccuSights at AccuSights LLC, Attn: Legal Notice, 2058 N. Western Ave, Chicago, IL 60647, with a copy by email to support@accusights.com with the subject line "ATTN: Legal Notice"; and (b) to Customer at the address and email in the Order Form. Notices are effective on receipt, or one business day after sending by email with confirmation of transmission (except notices of breach or termination, which must also be sent by courier or certified mail). Operational notices (Security Incidents, escalations, Portal notices, SLA and Exhibit A updates) may be given through the Portal and to Authorized Contacts by any method in the Escalation Matrix.

24.4 Electronic signatures and records. The Parties consent to transact electronically. This Agreement, Order Forms, amendments and acknowledgments may be executed by in-site electronic signature, by DocuSign or comparable service, or by exchange of signed PDF copies, each of which is an original, and the acceptance record described in the signature block is admissible evidence of execution. Counterparts together form one instrument.

24.5 Export; anti-corruption; government customers. Each Party will comply with applicable export-control and sanctions laws and anti-corruption laws. Customer will not enroll assets located in, or permit access to the Portal from, any country subject to comprehensive U.S. sanctions. If Customer is a government contractor, Customer acknowledges that AccuSights does not accept CUI by default (Section 7.5), and no FAR or DFARS clause flows down to AccuSights unless expressly accepted in an Order Form.

24.6 Force majeure. Neither Party is liable for delay or failure to perform (other than payment obligations) caused by events beyond its reasonable control, including natural disaster, epidemic, war, terrorism, civil unrest, labor dispute, governmental action, utility or internet failure, failure of a third-party platform on which the Services depend, and widespread or state-sponsored cyberattack not directed specifically at AccuSights' platform, provided the affected Party uses reasonable efforts to mitigate and resume performance.

24.7 Publicity. AccuSights may identify Customer by name and logo as a customer in its customer lists and marketing materials unless Customer opts out in writing; any quotation, case study or testimonial requires Customer's prior written approval.

24.8 Entire agreement; order of precedence. This Agreement (with its Exhibits, Order Forms, the DPA, any BAA and the incorporated Policies) is the entire agreement between the Parties regarding its subject matter and supersedes all prior or contemporaneous proposals, quotations, representations, marketing materials and agreements regarding the Protect Services and vCISO Services. In the event of conflict: (a) a BAA controls for PHI; (b) the DPA controls for personal information; (c) an Order Form controls to the extent it expressly varies this Agreement; (d) this Agreement controls over its Exhibits; and (e) the Exhibits control over the Policies.

24.9 Severability; waiver; construction. If any provision is held unenforceable, it will be enforced to the maximum extent permissible and the remainder will remain in effect; if a limitation in Section 13 is held unenforceable in part, the Parties intend that the court substitute the most protective enforceable limitation. No waiver is effective unless in writing, and no failure or delay is a waiver. Headings and the plain-language summary are for convenience only. "Including" means "including without limitation." This Agreement was negotiated by sophisticated commercial parties and is not to be construed against either Party as drafter.

24.10 Third-party beneficiaries. Except for AccuSights, Inc. under Sections 1.2, 1.3 and 14.2, and AccuSights' personnel under Section 13.7, there are no third-party beneficiaries of this Agreement.

Signatures

By signing below, each Party agrees to this Agreement, including its Exhibits, effective as of the Effective Date of the first Order Form.

ACCUSIGHTS LLC	
FIELD	ENTRY
SIGNATURE	_____
NAME	Samad Khan
TITLE	Chief Executive Officer
AUTHORITY	I represent that I am authorized to bind AccuSights LLC.
DATE / TIME (UTC)	_____
E-SIGNATURE RECORD	Method: ☐ In-site e-signature ☐ DocuSign ☐ Wet ink · Signer ID: _____ · IP: _____
RECORDED AUTOMATICALLY	_____ · Document version 2026.10 · SHA-256: _____

CUSTOMER: _____ (legal name, entity type and state of organization)	
FIELD	ENTRY
SIGNATURE	_____
NAME	_____
TITLE	_____
AUTHORITY	I represent that I am authorized to bind the Customer named above to this Agreement.
DATE / TIME (UTC)	_____
E-SIGNATURE RECORD	Method: ☐ In-site e-signature ☐ DocuSign ☐ Wet ink · Signer ID: _____ · Authenticated via MFA: ☐ · IP: _____ · User agent: _____ · Document version
RECORDED AUTOMATICALLY	2026.10 · SHA-256: _____

In-site e-signature note: the AccuSights platform records for each signature the authenticated signer identity, typed name and title, the authority representation, UTC timestamp, IP address, user agent, the document version and its SHA-256 hash, and the screen template presented, and emails an executed copy to both Parties. The exact text of each version, with its SHA-256 fingerprint, is archived at accusights.com/legal/archive and recorded in AccuSights' acceptance log at the time of acceptance. DocuSign or comparable services are used as a fallback for procurement processes that require an independent certificate of completion.

LIMITATION OF LIABILITY ACKNOWLEDGMENT

This acknowledgment is a separate, required act. It is not satisfied by signing the Agreement above.

The undersigned, on behalf of Customer, confirms that Customer has read and understood **Section 12.3 (No Guarantee of Detection, Prevention or Outcome)** and **Section 13 (Limitation of Liability)** of the AccuSights Protect Services Agreement, and specifically agrees that:

1. AccuSights LLC's total liability under the Agreement is limited to the greater of the fees paid for Protect (or, for vCISO claims, vCISO) in the prior twelve (12) months and \$1,000, unless a Security Breach Super-Cap is expressly elected in a signed Order Form;
2. ransom and extortion payments, breach-notification and credit-monitoring costs, forensic and recovery costs beyond the included scope, regulatory fines, business interruption, lost profits and third-party claims are excluded, however they are characterized;
3. AccuSights has no liability for Customer-Responsible Events, including declined or deferred recommendations recorded as Risk Acceptances, disabled or missing Agents, unpatched or end-of-life systems, phishing and credential compromise, and Sophisticated Attacks;
4. Service Credits are the sole and exclusive remedy for service-level failures;
5. AccuSights is not an insurer, and Customer will maintain at least \$1,000,000 of cyber-liability insurance; and
6. AccuSights, Inc. is not a party to, and has no liability under, the Agreement.



I acknowledge and agree to the Limitation of Liability on behalf of Customer.

Initials: _____ Name: _____ Title: _____

Date/time (UTC): _____

E-signature record: Signer ID _____ · IP _____ · Acknowledgment checkbox ID LOL-2026.10 · SHA-256 of Section 13 text _____

Exhibits (incorporated by reference):

- Exhibit A — Protect Service Description and SLA Schedule
- Exhibit B — vCISO Service Schedule
- Exhibit C — Shared Responsibility Matrix