

Exhibits A, B and C

Incorporated into the AccuSights Protect Services Agreement: the Protect Service Description and SLA Schedule, the vCISO Service Schedule and the Shared Responsibility Matrix.

Exhibit A	Service Description & SLA	Page 2
Exhibit B	vCISO Schedule	Page 11
Exhibit C	Shared Responsibility Matrix	Page 16

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

EXHIBIT A

Protect Service Description and SLA Schedule

ACCUSIGHTS LLC · VERSION 2026.10 — EFFECTIVE NOVEMBER 1, 2026

© 2026 AccuSights LLC. All rights reserved.

This Exhibit A is incorporated into the AccuSights Protect Services Agreement (the "Agreement"). Capitalized terms have the meanings in the Agreement. AccuSights may update this Exhibit under Section 22.2 of the Agreement (improvements permitted; no unilateral degradation during a Term).

A-1. Protect tiers and pricing

Tier names and list prices are those published at accusights.com/pricing as of the version date. The tier, User count and plan type (monthly or annual) stated in the Order Form control. Every tier is monitored 24x7x365 by the AccuSights SOC, with human acknowledgment of Severity-1 Security Incidents within 15 minutes and human triage within 60 minutes, around the clock. "Business Hours" means 8:00 a.m.–5:00 p.m. Central Time, Monday–Friday, excluding U.S. federal holidays.

	Protect Essentials	Protect Advanced	Protect Complete
LIST PRICE	\$25 per User / month	\$35 per User / month	\$50 per User / month
MINIMUM USERS	10	10	10
PLANS AVAILABLE	Monthly or annual	Monthly or annual	Monthly or annual
DESCRIPTION	Managed detection and response on every endpoint, inbox, identity and cloud account, with automatic containment per the elected Response Mode.	Everything in Protect Essentials plus network, perimeter and web-property telemetry sources, faster human review of Sev-2 and Sev-3 cases, and a quarterly service review.	Everything in Protect Advanced plus a named Cyber Success Engineer, a monthly service review, and priority scheduling for onboarding, tuning and scope changes.
AUTOMATED DETECTION AND CONTAINMENT (PER RESPONSE MODE)	24x7x365	24x7x365	24x7x365
SOC MONITORING AND HUMAN ANALYST COVERAGE FOR SEV-1	24x7x365	24x7x365	24x7x365
HUMAN ACKNOWLEDGMENT OF SEV-1 (≤ 15 MINUTES) AND HUMAN TRIAGE (≤ 60 MINUTES)	24x7x365	24x7x365	24x7x365

	Protect Essentials	Protect Advanced	Protect Complete
HUMAN CONFIRMATION CALL ON SEV-1	24x7x365	24x7x365	24x7x365
TELEMETRY SOURCE CLASSES (SEE A-2)	Endpoint, identity, email, cloud tenant	All Essentials sources plus network / perimeter, web properties, backup and other log sources	All Advanced sources
SEV-2 HUMAN TRIAGE	Within 1 Business Day	Within 4 Business Hours	Within 4 Business Hours
SEV-3 HUMAN REVIEW	Within 3 Business Days	Within 1 Business Day	Within 1 Business Day
NAMED CYBER SUCCESS ENGINEER	Not included (SOC case team and Portal)	Not included (SOC case team and Portal)	Included
SERVICE REVIEW	Annual (at renewal)	Quarterly	Monthly
TYPICAL FIT	Every business	Businesses with firewalls, public web properties or multiple sites that want fuller source coverage and faster follow-up on lower-severity cases	Healthcare, legal, financial, defense suppliers and multi-location businesses that want a named engineer who knows their environment

Included in every tier:

- Security awareness and phishing training for staff, scored per person and per team, no per-module charges
- Dark-web monitoring for Customer's domain(s) and personnel credentials
- Device management and patching support for enrolled endpoints (patch deployment is a shared responsibility; see Exhibit C)
- Vulnerability scanning of In-Scope Assets, monthly and on material change
- One-page monthly report
- Compliance evidence produced from Protect activity, mapped to Customer's frameworks in the Portal

Billing unit. A "User" is each individual with an active mailbox or identity in the connected identity/email tenant, or each individual assigned an enrolled endpoint, whichever is greater. Shared devices, servers and service accounts are covered without a separate User charge up to a ratio of two (2) enrolled servers or shared devices per User; above that ratio, additional devices are billed at the per-device rate stated in the Order Form.

A-2. Monitoring stack (generic description)

The Protect Services collect Telemetry from, and where authorized act on, the following source classes. Specific products are selected by AccuSights and may change under Section 4.4 of the Agreement.

SOURCE CLASS	WHAT IS COLLECTED	RESPONSE ACTIONS AVAILABLE (AUTHORIZE / COLLABORATE MODES)
Endpoint Agent (Windows, macOS, supported Linux; mobile via MDM where supported)	Process, file, registry, network and user-session events; installed software and patch state; device posture	Host isolation; process termination; file quarantine; remote wipe of enrolled managed devices where MDM-integrated
Identity (Microsoft Entra ID / Microsoft 365, Google Workspace; other IdPs on request)	Sign-in and audit logs, MFA events, risky-user signals, privilege changes, app consents	Disable account; revoke sessions and refresh tokens; force password reset; remove malicious OAuth grants
Email (Microsoft 365 Exchange Online, Google Workspace Gmail)	Message metadata and headers, mail-flow and inbox-rule changes, URL/attachment verdicts, user-reported phishing	Remove malicious inbox/forwarding rules; purge or quarantine messages; block sender/domain
Cloud (Microsoft 365 tenant, Google Workspace tenant; Azure, AWS, GCP control-plane logs where connected)	Admin and configuration audit logs, sharing events, storage access events	Disable compromised keys/service principals where connected; block indicators
Network / perimeter (supported firewalls, DNS filtering, Wi-Fi controllers where integrated)	Flow logs, DNS queries, IDS alerts, VPN authentication	Block IP/domain at firewall or DNS filter where integration supports it
Web properties (Customer's public websites and stores)	External attack-surface scanning, admin-login anomalies where plugin/agent supports it, certificate and DNS changes	Notify only (no Response Actions) unless Playbook states otherwise
Backup and other log sources	Backup job success/failure where integrated; other syslog sources by agreement	Notify only

Telemetry is transmitted encrypted to AccuSights' platform hosted in the United States (Microsoft Azure, primary region East US 2, and Amazon Web Services US regions) and retained for 90 days on every tier as stated in Sections 18.3 and 18.10 of the Agreement. There is no archival tier and no extended-retention option.

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 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. The 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 90-day window on request at its then-current hourly rate, and has no liability for the unavailability of telemetry older than 90 days.

A-3. Severity definitions

AccuSights assigns Severity at triage and may re-classify as facts develop. Severity drives the SLA targets in A-4.

SEVERITY	DEFINITION	EXAMPLES
Sev 1 — Critical	Confirmed or highly probable active compromise with imminent risk of material harm to In-Scope Assets or Customer Data	Active ransomware encryption; confirmed attacker interactive session on a server or privileged account; confirmed business-email-compromise with financial redirection in progress; mass data exfiltration in progress
Sev 2 — High	Probable compromise or high-confidence malicious activity that is contained or not yet impacting operations, or a critical exposure requiring urgent action	Malware executed and quarantined by Agent; successful sign-in from anomalous location on a standard user account; credentials for Customer's domain found on the dark web with evidence of active use; critical unpatched internet-facing vulnerability with active exploitation in the wild
Sev 3 — Medium	Suspicious activity requiring investigation, or policy/hygiene issue with meaningful risk	Blocked phishing campaign targeting multiple users; MFA fatigue attempts; new admin account created outside change window; Agent offline on a server for more than 24 hours
Sev 4 — Low / Informational	Low-risk detections, tuning items and informational findings	Blocked commodity malware download; benign-verified anomaly; vulnerability scan findings without known exploitation; awareness-training results

Detection time. "Detection" for SLA purposes is the timestamp at which the AccuSights platform generates the alert that is subsequently classified as the Security Incident, not the time the underlying event occurred on Customer's system.

Acknowledgment. "Acknowledgment" means a human analyst has opened or taken ownership of the case, assigned Severity, initiated any automated Response Action permitted by the Response Mode and Playbook, and sent notice to the Authorized Contacts by the Sev-1 channel in the Escalation Matrix. The platform may open the case and send the first notice automatically, but the Sev-1 acknowledgment SLA is met only when a human analyst has taken ownership within the target time.

Triage. "Triage" means a human analyst has reviewed the case, confirmed or revised Severity, determined initial scope, and communicated findings and recommended or executed Response Actions to the Authorized Contacts.

A-4. Service-level targets

All targets run from the Monitoring Start Date. Times are elapsed from Detection.

METRIC	TARGET	APPLIES TO	COVERAGE
Sev-1 acknowledgment (human)	≤ 15 minutes	All tiers	24x7x365
Sev-1 triage (human)	≤ 60 minutes	All tiers	24x7x365
Sev-2 acknowledgment	≤ 60 minutes	All tiers	24x7x365 (automated)
Sev-2 triage	Protect Essentials: within 1 Business Day; Protect Advanced and Protect Complete: ≤ 4 Business Hours (targets, no credit)	All tiers	Business Hours
Sev-3 / Sev-4	Protect Essentials: reviewed within 3 Business Days; Protect Advanced and Protect Complete: within 1 Business Day; Sev-4 included in weekly digest (targets, no credit)	All tiers	Business Hours
Portal availability	99.5% per calendar month, excluding scheduled maintenance (≤ 8 hours/month, notified ≥ 48 hours ahead, outside Business Hours where practicable) and emergency maintenance	All tiers	Measured by AccuSights monitoring
Monthly report	Delivered by the 10th of the following month (target, no credit)	All tiers	—

Only the Sev-1 acknowledgment metric and Portal availability carry Service Credits. All other targets are operational objectives.

A-5. Service Credit table

FAILURE	CREDIT	CAP
Each Sev-1 Security Incident not acknowledged within 15 minutes	5% of that month's Protect Fees per missed event	
Portal availability below 99.5% but ≥ 99.0% in a month	5% of that month's Protect Fees	Aggregate credits for all failures in a month: 25% of that month's Protect Fees
Portal availability below 99.0% in a month	10% of that month's Protect Fees	

Claim window: 30 days after the end of the month (Agreement §8.3). **Exclusions:** Agreement §8.4 (pre-Monitoring Start Date; Customer-Responsible Events; maintenance; force majeure; third-party platform outages; suspension; payment breach). **Sole remedy:** Agreement §8.5.

Chronic failure termination right. If AccuSights misses the Sev-1 acknowledgment target for three (3) or more Sev-1 Security Incidents in each of three (3) consecutive months, in each case not excused under §8.4, Customer may terminate the affected Order Form on thirty (30) days' notice given within thirty (30) days after the third month, with a pro-rata refund of prepaid unused Fees. This is the only termination right arising from service-level performance.

A-6. Included vs. add-on services

SERVICE	INCLUDED	ADD-ON (ORDER FORM OR HOURLY)
Continuous monitoring, detection, case management	All tiers	—
Automated containment per Response Mode	All tiers	—
Human Sev-1 acknowledgment, triage and Response Action execution, 24x7x365	All tiers	—
Incident scoping, initial containment guidance and forensic triage	Up to 8 analyst hours per incident, all tiers	Forensic investigation beyond the 8 included hours per incident: priced on the Order Form (hourly rate or prepaid block)
Forensic investigation (disk/memory imaging, timeline reconstruction, root-cause report) beyond the 8 included hours per incident	Not included	Priced on the Order Form
Incident-response retainer (prepaid response hours with a committed response window)	Not included	Priced on the Order Form
Regulatory response support (regulator, auditor, prime-contractor or insurer inquiries arising from a Security Incident; declarations, record production, interviews; Agreement §23.8)	Not included	Priced on the Order Form; otherwise at AccuSights' then-current hourly rate
Restoration, rebuild and recovery of systems and data	Not included (Customer / Customer's MSP)	Professional services at hourly rates
Breach coaching, legal, notification, credit monitoring, PR	Not included (Customer's insurer / counsel)	Not offered; AccuSights can refer to Customer's carrier panel

SERVICE	INCLUDED	ADD-ON (ORDER FORM OR HOURLY)
Security awareness and phishing training	All tiers	—
Dark-web monitoring (Customer domains and personnel credentials)	All tiers, up to 3 Customer domains	Additional domains: priced on the Order Form
Vulnerability scanning of In-Scope Assets (monthly and on change)	All tiers	Authenticated internal scanning or penetration testing: quoted separately
Device management and patching support	All tiers (see Exhibit C for split)	Full managed patching where no Customer's MSP exists: quoted separately
Compliance evidence mapped to frameworks	All tiers	Framework readiness, policies, audits: AccuSights, Inc. Comply / Assess under separate agreement
Telemetry retention	90 days on all tiers (secondary, read-only working copies; Agreement §18.10)	Not offered. There is no extended-retention add-on and no archival tier; Customer retains its own logs and records for the periods required by CMMC / NIST SP 800-171 (AU family), HIPAA, PCI DSS, its insurer and litigation holds. Export assistance for data still within the 90-day window at AccuSights' then-current hourly rate.
Onboarding and baseline	Included (remote)	On-site deployment: quoted
Tabletop exercise	Not included (included in vCISO Program and Executive packages, Exhibit B)	Quoted per exercise
CUI-scoped enclave monitoring	Not included	Separate CUI-scoped Order Form required (Agreement §7.5)
BAA with AccuSights LLC for Customers that are HIPAA covered entities or business associates	Included at no charge; must be executed before the Monitoring Start Date	—

A-7. Reporting cadence

REPORT	FREQUENCY	AUDIENCE	CONTENT
Real-time alerts and case updates	As they occur	Authorized Contacts per Escalation Matrix	Severity, affected assets, actions taken, actions requested
Sev-1 incident summary	Within 1 Business Day of containment	Authorized Contacts, executive sponsor	What happened, what was done, when; open items; Risk Acceptances created

REPORT	FREQUENCY	AUDIENCE	CONTENT
Weekly digest	Weekly (email)	Security contact / Customer's MSP	Sev-2 to Sev-4 case summary, Agent health, open vulnerabilities, awareness-training status
One-page monthly report	By the 10th of the following month	Owner / executive sponsor	Incidents by Severity, SLA performance and any credits, coverage metrics (Agent %, MFA %, patch compliance), open Risk Acceptances, top recommendations
Compliance evidence export	Continuous in Portal; on request	Customer's compliance lead / auditor	Dated evidence of Protect controls mapped to Customer's frameworks (informational only; Agreement §12.3(e))
Service review	Annual at renewal (Protect Essentials); quarterly (Protect Advanced); monthly (Protect Complete)	Customer leadership; SOC case team (Essentials and Advanced) or named Cyber Success Engineer (Complete)	Trend review, tuning, scope changes, renewal planning

A-8. Escalation matrix template

Customer completes and maintains this in the Portal (Agreement §7.1(g)). At least two Authorized Contacts must be reachable 24x7 by phone.

ROLE	NAME	TITLE	PHONE (24X7)	ALTERNATE CHANNEL (SMS / SIGNAL / TEAMS)	EMAIL	HOURS AVAILABLE	AUTHORITY
Primary Sev-1 contact						24x7	☐ Approve Response Actions ☐ Change Response Mode ☐ Approve Playbooks
Secondary Sev-1 contact						24x7	☐ Approve Response Actions ☐ Change Response Mode ☐ Approve Playbooks
Executive sponsor / owner							☐ Change Response Mode ☐ Accept Risk
IT lead or Customer's MSP contact							☐ Approve Response Actions ☐ Execute Collaborate-mode actions
Compliance / privacy lead (HIPAA Security Official, etc.)							☐ Receive breach-relevant notices
Cyber insurance carrier / breach coach (for Customer's own use)							Reference only

Escalation sequence (Sev-1): Platform notice to Primary and Secondary by phone call and alternate channel at acknowledgment → if no response in 15 minutes, Executive sponsor → if no response in 30 minutes, all contacts on rotation every 30 minutes, documented in the case. In Authorize mode, containment proceeds in parallel; in Collaborate mode, no Response Action is taken until an authorized contact approves; in Notify mode, no Response Action is taken.

AccuSights contacts: SOC hotline +1 (773) 747-7490 (24x7x365) · support@accusights.com with subject line "ATTN: SOC" · Portal case system · Named Cyber Success Engineer (Protect Complete; assigned at onboarding).

A-9. Onboarding checklist and Monitoring Start Date

STEP	OWNER	PREREQUISITE TO MONITORING START DATE?
Order Form executed; cap acknowledgment recorded	Both	Yes
BAA with AccuSights LLC executed (required for Customers that are HIPAA covered entities or business associates)	Both	Yes, for HIPAA covered entities and business associates
Asset inventory completed in Portal	Customer / Customer's MSP	Yes
Endpoint Agent deployed on ≥ 95% of inventoried endpoints and servers, reporting healthy	Customer / Customer's MSP (AccuSights assists)	Yes
Identity and email tenant integrations connected with required permissions	Customer / Customer's MSP	Yes
Cloud, network and web integrations connected (as applicable to tier)	Customer / Customer's MSP	Recommended; gaps logged as Risk Acceptances
Escalation Matrix completed with ≥ 2 contacts reachable 24x7	Customer	Yes
Response Mode confirmed and initial Playbooks approved	Customer	Yes
Baseline and tuning period completed (≥ 7 days)	AccuSights	Yes
Monitoring Start Date declared in Portal	AccuSights	—
100% Agent coverage achieved	Customer / Customer's MSP	Within 30 days after Monitoring Start Date

EXHIBIT B

vCISO Service Schedule

ACCUSIGHTS LLC · VERSION 2026.10 — EFFECTIVE NOVEMBER 1, 2026

© 2026 AccuSights LLC. All rights reserved.

This Exhibit B is incorporated into the AccuSights Protect Services Agreement (the "Agreement") and applies only if a vCISO package is ordered in an Order Form. Capitalized terms have the meanings in the Agreement. Section 9 of the Agreement governs the vCISO Services and controls over this Exhibit.

B-1. Packages

All packages are delivered remotely by a named lead vCISO with support from AccuSights' advisory team. Hours are monthly allocations of advisory time, including meetings, document preparation, review and correspondence. Package prices and the hourly overage rate are stated on the Order Form.

	vCISO Advisory	vCISO Program	vCISO Executive
MONTHLY HOURS	8 hours / month	16 hours / month	32 hours / month
MONTHLY FEE	As stated on the Order Form	As stated on the Order Form	As stated on the Order Form
TYPICAL FIT	Businesses that need a standing security advisor, policy owner and a quarterly leadership briefing	Businesses building or maturing a security program against a framework (CMMC, HIPAA, SOC 2, ISO 27001, PCI DSS) with audit or assessment ahead	Regulated or multi-site businesses needing near-weekly executive engagement, board reporting and vendor/customer-facing security leadership support
CADENCE	Monthly working session (60 min) + ad hoc	Bi-weekly working sessions + monthly leadership check-in	Weekly working sessions + monthly leadership briefing + quarterly board/owner briefing
ROLL-OVER	Unused hours do not roll over	Unused hours do not roll over	Unused hours do not roll over
OVERAGE	Hourly rate stated on the Order Form, pre-approved by an Authorized Contact	Hourly rate stated on the Order Form, pre-approved by an Authorized Contact	Hourly rate stated on the Order Form, pre-approved by an Authorized Contact
TERM	Annual plan (12 months) or monthly plan, as stated on the Order Form (Agreement §15.2)	Annual plan (12 months) or monthly plan, as stated on the Order Form (Agreement §15.2)	Annual plan (12 months) or monthly plan, as stated on the Order Form (Agreement §15.2)
REQUIRES PROTECT SUBSCRIPTION?	No; may be ordered with or without Protect	No; may be ordered with or without Protect	No; may be ordered with or without Protect

Hours are tracked in the Portal and reported monthly. Time is recorded in 15-minute increments. Travel, if requested and approved, is billed at hourly rates plus expenses.

B-2. Deliverables by package

Deliverables are recommendations and work product for Customer's internal use (Agreement §§9.5, 9.7). Frequency shown is the default; Customer may re-prioritize within the monthly hours.

DELIVERABLE	ADVISORY	PROGRAM	EXECUTIVE
Security program roadmap — 12-month prioritized plan mapped to Customer's chosen framework(s), with owners, effort estimates and dependencies	Annual (light)	Annual, reviewed quarterly	Annual, reviewed monthly
Risk register — maintained list of identified risks, likelihood/impact ratings, treatment decisions and open Risk Acceptances (Agreement §10)	Reviewed quarterly	Reviewed monthly	Reviewed monthly
Policy review and drafting — review of existing policies; drafting or updating from AccuSights templates (information security, acceptable use, access control, incident response, backup, vendor management, etc.)	Up to 4 policies / year	Up to 10 policies / year	Full policy set maintained
Leadership / board briefing — written summary and live presentation of posture, incidents, risk trends, roadmap status and budget needs	Quarterly (written)	Quarterly (written + live)	Monthly written; quarterly live board/owner briefing
Vendor and third-party risk — questionnaire review, risk tiering, contract security-clause guidance for Customer's key vendors	Up to 5 vendors / year	Up to 15 vendors / year	Ongoing, up to 30 vendors / year
Customer / prime security questionnaire support — drafting responses for Customer's officers to review, approve and sign	Up to 2 / year	Up to 6 / year	Ongoing
Incident response plan — plan development or refresh aligned to Protect Response Modes and Playbooks	Review only	Develop or refresh annually	Develop or refresh annually
Tabletop exercise — facilitated scenario exercise for leadership and IT, with after-action report	Not included (add-on)	Annual	Semi-annual
Audit and assessment support — readiness planning, evidence organization, assessor-liaison coaching, remediation tracking (preparatory only; Agreement §9.9)	Not included (add-on)	Included for one framework / year	Included for up to two frameworks / year
Cyber-insurance application support — assistance preparing control information for Customer's broker; Customer's officer signs	Included	Included	Included

DELIVERABLE	ADVISORY	PROGRAM	EXECUTIVE
Security awareness program oversight — review of Protect training results, targeted campaigns	Included	Included	Included
Budget and staffing guidance — security spend benchmarking, tooling rationalization, hiring profiles	On request within hours	Annual	Semi-annual
Metrics dashboard — KPI set (Agent coverage, MFA, patch compliance, phishing rate, open risks) reported monthly	—	Included	Included
Executive representation — participation in Customer's leadership meetings, customer or prime security calls, and regulator or auditor meetings as Customer's advisor (never as Customer's officer or signatory)	Not included	Up to 2 events / quarter	Up to 2 events / month

B-3. Exclusions

The vCISO Services do not include, and AccuSights will not perform under a vCISO package:

1. Acting as Customer's HIPAA Security Official or Privacy Official, CMMC Affirming Official, SEC disclosure signatory, Data Protection Officer, PCI responsible officer, 23 NYCRR 500 / FTC Safeguards "Qualified Individual," or any other statutory, regulatory, contractual or fiduciary role (Agreement §9.3).
2. Signing, certifying, attesting, affirming, submitting or filing any assessment, self-assessment, SPRS score, attestation of compliance, regulatory filing, insurance application, security questionnaire, contract representation or public statement (Agreement §9.4).
3. Legal advice, legal opinions or interpretation of law for Customer; Customer should consult its own counsel.
4. Audit, attestation or certification services (SOC 2, ISO 27001, PCI ROC, CMMC certification assessment), or participation in Customer's CMMC Level 2 certification assessment within three years of consulting (Agreement §9.9).
5. Hands-on engineering, system administration, configuration changes, patching or implementation of controls on Customer's systems (available from AccuSights or Customer's MSP under separate scope).
6. Incident response operations, forensic investigation, breach notification, or crisis communications (see Exhibit A add-ons and Customer's cyber-insurance carrier); the vCISO may advise Customer's incident commander within package hours.
7. Penetration testing, red-team exercises, code review or application security testing.
8. Compliance-readiness projects, evidence collection platforms and continuous-compliance subscriptions offered by AccuSights, Inc. (Assess, Comply, CMMC Accelerator), which are ordered separately from AccuSights, Inc.
9. Supervision, management, hiring, discipline or performance review of Customer personnel; approval of Customer expenditures; or execution of contracts on Customer's behalf.
10. Services to Customer's affiliates, customers or partners, unless named in the Order Form.
11. On-site attendance, unless ordered and billed separately.

12. Any guarantee that Customer will be free of security incidents, will pass any audit or assessment, or is or will be compliant with any law, regulation or framework (Agreement §12.3).

B-4. Working assumptions

- Customer designates an executive sponsor and an internal point of contact with authority to schedule sessions, provide information and make decisions.
- Customer provides timely access to documents, systems (read-only where required), personnel and its Customer's MSP.
- AccuSights may use its templates, tools and AI-assisted drafting to produce deliverables; all deliverables are reviewed by the lead vCISO before delivery. AI outputs are reviewed by AccuSights personnel and may be inaccurate; Customer's management reviews before adoption.
- Sessions are held remotely by video during Business Hours (8:00 a.m.–5:00 p.m. Central Time, Monday–Friday).
- Package changes (upgrade at any time; downgrade at renewal) are made by Order Form addendum.

B-5. Acknowledgments (short form, for signature with the Order Form)

Customer's signatory confirms, on behalf of Customer, that Customer understands and agrees:

1. **Advisory only.** The vCISO Services are advice and recommendations. Customer's management decides what to adopt, fund and implement, and is responsible for the outcome. (Agreement §§9.2, 9.5)
2. **Not an officer or employee.** The vCISO is not Customer's officer, director, employee or agent, holds no corporate office, and has no authority to bind Customer or direct its personnel. The "CISO" title is descriptive of the service only. (Agreement §9.2)
3. **Not a statutory role.** The vCISO is not Customer's HIPAA Security Official, CMMC Affirming Official, DPO, SEC disclosure signatory or any other statutory or regulatory official, unless a named individual separately accepts such a role in a signed Order Form. (Agreement §9.3)
4. **No signing or attesting.** The vCISO will not sign, certify, attest to, affirm, submit or file any assessment, score, filing, questionnaire or public statement on Customer's behalf. (Agreement §9.4)
5. **No fiduciary duty; no third-party reliance.** No fiduciary relationship is created, and no third party may rely on vCISO deliverables. Customer will not hold AccuSights out as having certified or assumed responsibility for its security or compliance. (Agreement §§9.6, 9.7)
6. **Not a certifier.** AccuSights is not a C3PAO, auditor, CPA firm, QSA or certification body and does not guarantee any audit, assessment or compliance outcome. (Agreement §9.9)
7. **Non-exclusive.** AccuSights may serve other clients, including Customer's competitors. (Agreement §9.8)
8. **Liability.** The Limitation of Liability in Section 13 of the Agreement applies to the vCISO Services, measured against vCISO Fees (the greater of the vCISO fees paid in the prior 12 months and \$1,000).
9. **Hours.** Unused hours do not roll over; hours beyond the monthly allocation are billed at the hourly rate on the Order Form.

☐ I acknowledge the vCISO terms above on behalf of Customer.

Initials: _____ Name: _____ Title: _____

Date/time (UTC): _____

E-signature record: Signer ID _____ · IP _____ · Acknowledgment checkbox ID VCISO-2026.10 · SHA-256

EXHIBIT C

Shared Responsibility Matrix

ACCUSIGHTS LLC · VERSION 2026.10 — EFFECTIVE NOVEMBER 1, 2026

© 2026 AccuSights LLC. All rights reserved.

This Exhibit C is incorporated into the AccuSights Protect Services Agreement (the "Agreement"). It records which party is responsible for each activity needed for the Protect Services to work. A responsibility assigned to "Customer" is Customer's whether Customer performs it directly or through Customer's MSP; where Customer has no MSP, the "Customer's MSP" column responsibilities fall to Customer. A failure in a Customer or Customer's MSP responsibility that contributes to a Security Incident or loss is a Customer-Responsible Event (Agreement §13.4).

LEGEND: **R** = Responsible (performs the activity) **A** = Approves / decides
S = Supports (assists, advises, provides tooling or guidance) **I** = Informed — = No role

C-1. Onboarding

#	RESPONSIBILITY	ACCUSIGHTS LLC	CUSTOMER	CUSTOMER'S MSP (IF ANY)
1	Execute Order Form, cap acknowledgment and, for Customers that are HIPAA covered entities or business associates, the BAA with AccuSights LLC (before the Monitoring Start Date)	R	R A	I
2	Provide complete and accurate asset inventory (endpoints, servers, identities, tenants, cloud accounts, network devices, web properties, remote/BYOD devices used for business)	S	A	R
3	Confirm ownership of, and authority to monitor and act on, every In-Scope Asset, including third-party-hosted and BYOD assets (Agreement §6.5)	I	R A	S
4	Provide Agent packages, deployment instructions and integration guides	R	I	I
5	Deploy endpoint Agents to ≥ 95% of inventoried endpoints and servers before Monitoring Start Date, and 100% within 30 days after	S	A	R
6	Grant identity, email, cloud and network integration permissions at the scopes AccuSights specifies	S	A	R
7	Complete Escalation Matrix with ≥ 2 Authorized Contacts reachable 24x7	S	R A	S

#	RESPONSIBILITY	ACCUSIGHTS LLC	CUSTOMER	CUSTOMER'S MSP (IF ANY)
8	Elect Response Mode (Notify / Collaborate / Authorize) in the Order Form; designate excluded assets (life-safety, clinical, production-control)	S	R A	S
9	Draft initial Playbooks (conditions, permitted Response Actions, decision windows)	R	A	S
10	Provide employee notices and obtain consents required for endpoint, email and identity monitoring under applicable law and Customer's policies	—	R A	S
11	Disclose regulated-data environments (PHI, CUI, PCI cardholder data) and ensure BAA or CUI-scoped order is in place before enrollment	I	R	S
12	Complete baseline and detection tuning; declare Monitoring Start Date	R	I	I
13	Provide Portal training to Authorized Contacts	R	I	I

C-2. Steady state — detection and response

#	RESPONSIBILITY	ACCUSIGHTS LLC	CUSTOMER	CUSTOMER'S MSP (IF ANY)
14	Collect, store and analyze Telemetry 24x7x365; maintain detection content and threat intelligence	R	—	—
15	Triage Security Events, assign Severity, open and manage cases	R	I	I
16	Acknowledge and escalate Sev-1 Security Incidents per Exhibit A and the Escalation Matrix	R	I	I
17	Respond to escalations within the Playbook decision window; approve or decline Response Actions (Collaborate mode)	I	R A	S
18	Execute Response Actions in Authorize mode within approved Playbooks	R	I	I
19	Execute recommended Response Actions in Notify and Collaborate modes	S	A	R

#	RESPONSIBILITY	ACCUSIGHTS LLC	CUSTOMER	CUSTOMER'S MSP (IF ANY)
20	Reverse containment (un-isolate, re-enable) once threat contained, on Authorized Contact request	R	A	S
21	Restore data and rebuild systems after an incident; recover from backups	S (add-on)	A	R
22	Report suspected incidents, lost devices and credential compromise to AccuSights within 24 hours; preserve evidence	I	R	R
23	Engage cyber-insurance carrier, breach coach, counsel, notification vendors; make breach-notification decisions and filings	I	R A	—
24	Forensic investigation beyond included triage scope	R (add-on)	A	S
25	Implement remediation recommendations within stated timeframes, or record a Risk Acceptance	S	A	R
26	Maintain and review Risk Acceptance log; revisit accepted risks	R (log)	A	I

C-3. Steady state — security hygiene and environment

#	RESPONSIBILITY	ACCUSIGHTS LLC	CUSTOMER	CUSTOMER'S MSP (IF ANY)
27	Keep Agents installed, healthy and reporting on 100% of in-scope endpoints; enroll new devices within 5 business days; restore offline Agents	S (health alerts)	A	R
28	Enforce MFA on all administrative, privileged, remote-access and email accounts	S (alerts, guidance)	A	R
29	Patch critical vulnerabilities (CVSS ≥ 9.0 / vendor-critical) within 30 days; other patches within a reasonable time	S (scanning, patch deployment support per tier)	A	R
30	Retire or isolate end-of-life and unsupported systems, or record Risk Acceptance	S	A	R

#	RESPONSIBILITY	ACCUSIGHTS LLC	CUSTOMER	CUSTOMER'S MSP (IF ANY)
31	Maintain immutable or offline backups of business-critical data; test restoration at least quarterly	S (backup-job alerts where integrated)	A	R
32	Manage identity provider, email tenant, cloud tenant and network configuration; implement AccuSights hardening recommendations	S	A	R
33	Network segmentation, firewall rules, Wi-Fi and terminal isolation	S	A	R
34	Endpoint encryption, MDM enrollment and device management policies	S (device management support per tier)	A	R
35	Privileged-access management, admin account lifecycle, joiner/mover/leaver process	S	A	R
36	Keep asset inventory and Escalation Matrix current (within 1 business day of changes)	S	A	R
37	Notify AccuSights before material environment changes (tenant migration, IdP change, EDR change, new site)	I	R	R
38	Vulnerability scanning of In-Scope Assets (monthly and on change) and reporting	R	I	I
39	Security awareness and phishing training delivery and scoring	R	A (participation)	I
40	Dark-web monitoring for Customer domains and credentials; alerting on exposure	R	A (password resets)	R (resets)
41	Website, e-commerce and plugin patching; admin credential hygiene for web properties	S (external monitoring)	A	R

C-4. Data, compliance and governance

#	RESPONSIBILITY	ACCUSIGHTS LLC	CUSTOMER	CUSTOMER'S MSP (IF ANY)
42	Secure AccuSights' own platform, Telemetry storage and personnel access (Agreement §18.6)	R	—	—

#	RESPONSIBILITY	ACCUSIGHTS LLC	CUSTOMER	CUSTOMER'S MSP (IF ANY)
43	Retain secondary, read-only copies of Telemetry for 90 days per Exhibit A and Agreement §18.10; export and delete Customer Data at termination per Agreement §17	R	A (export requests)	S
43a	Log and records retention (Not a SIEM; Secondary Logs): retain Customer's own logs and records for the periods required by CMMC / NIST SP 800-171 (AU family), HIPAA, PCI DSS, Customer's insurer, litigation holds or any other obligation; maintain Customer's own system of record; request export of any Telemetry still within the 90-day window	S (export assistance at hourly rate, within the 90-day window only)	R A	R
44	Classify and control regulated data on Customer systems (PHI, CUI, PCI); keep it out of unscoped environments	—	R	S
45	Compliance evidence: AccuSights produces evidence of Protect controls; Customer owns its compliance program, assessments, attestations and filings	R (evidence)	R A (program)	S
46	Regulatory, auditor, prime-contractor and insurer communications, questionnaires and attestations	S (hourly / vCISO)	R A	S
47	Maintain cyber-liability insurance ≥ \$1,000,000 per claim; provide certificate on request	I	R	—
48	Maintain AccuSights E&O / cyber insurance per Agreement §20.1	R	I	—
49	Manage subcontractors and tooling vendors used to deliver Protect; remain responsible for their performance	R	I	—
50	Manage Customer's other vendors (including Customer's MSP) and their access to Customer systems	—	R A	R (own access)
51	Agent removal and integration revocation at offboarding (within 30 days)	S (instructions, remote disable)	A	R

C-5. Notes

- **MSP-purchased Protect.** Where Customer's MSP places the order, the Agreement is accepted by Customer (the end client) directly or by the MSP holding written authority to bind Customer (Agreement §3.4). The MSP may bill Customer at wholesale and remains responsible for collection from Customer. The MSP's column responsibilities are contractual obligations of the MSP to Customer, and Customer remains responsible to AccuSights for them under Agreement §5.5.

- **Coverage.** AccuSights "R" entries for Sev-1 human acknowledgment, triage and Response Action execution apply 24x7x365 on all tiers. Human review of Sev-2 to Sev-4 cases follows the Business Hours windows for Customer's tier in Exhibit A. Automated detection and containment operate 24x7x365 on all tiers.
- **Changes.** The Parties may re-allocate individual rows for a Customer by Order Form. Absent that, this Exhibit controls.
- **Read with Exhibit A (Service Description) and Agreement Sections 6 (Response Modes), 7 (Customer Obligations), 10 (Risk Acceptance) and 13.4 (Customer-Responsible Events).**