WEBSITE TERMS OF USE

Your use of this website, including any content, functionality, and services offered on or through https://cpcyber.com/ (this "**Site**"), is subject to the following Terms of Use. Please read the Terms of Use carefully before you start using the Site. By using the Site, you accept and agree to be bound and abide by these terms and our Privacy Policy below. If you do not accept and agree to these Terms of Use, do not use the Site.

We may revise and update these Terms of Use from time to time in our sole discretion. All changes are effective immediately when we post them. Your continued use of the Site following the posting of revised Terms of Use means that you accept and agree to the changes.

The Site and its entire contents, features, and functionality (including but not limited to all information, software, text, displays, images, video, and audio, and the design, selection, and arrangement thereof) are owned by us, our licensors, or other providers of such material and are protected by United States and international copyright, trademark, patent, trade secret, and other intellectual property or proprietary rights laws.

The information presented on or through the Site is made available solely for general information purposes. We do not warrant the accuracy, completeness, or usefulness of this information. Any reliance you place on such information is strictly at your own risk. We disclaim all liability and responsibility arising from any reliance placed on such materials by you or any other visitor to the Website, or by anyone who may be informed of any of its contents.

This Site may include content provided by third parties. All statements and/or opinions expressed in these materials are solely the opinions and the responsibility of the person or entity providing those materials. We are not responsible, or liable to you or any third party, for the content or accuracy of any materials provided by any third party.

STANDARD TERMS

These Standard Terms apply to the Strategic Cybersecurity Services Master Services Agreement and any SOWs between Cornerstone Partners, LLC d/b/a CP Cyber ("**CP Cyber**") and its clients. By agreeing to the Strategic Cybersecurity Services Master Services Agreement or any SOW, clients agree to these Standard Terms. Capitalized terms used in these Standard Terms and not otherwise defined have the meanings assigned to them in the applicable Strategic Cybersecurity Services Master Services Agreement or SOW. These Standard Terms and the Strategic Cybersecurity Services Master Services Agreement or SOW between CP Cyber and the applicable client are referred to herein collectively as, the "**Agreement**."

1. Client Obligations. Client shall:

a. cooperate with CP Cyber in all matters relating to the Services and appoint a Client employee to serve as the primary contact with respect to this Agreement and who will have the authority to act on behalf of Client with respect to matters pertaining to this Agreement;

b. provide such access to Client's premises and such office accommodation and other facilities as may reasonably be requested by CP Cyber, for the purposes of performing the Services;

c. respond promptly to any CP Cyber request to provide direction, information, approvals, authorizations, or decisions that are reasonably necessary for CP Cyber to perform Services in accordance with the requirements of this Agreement;

d. provide such information as CP Cyber may request, in order to carry out the Services, in a timely manner, and ensure that it is complete and accurate in all material respects; Client further acknowledges and warrants that CP Cyber shall be entitled in all respects to rely on the accuracy and completeness of any materials provided to it by Client hereunder;

e. ensure that all Client equipment is in good working order and suitable for the purposes for which it is used in relation to the Services and conforms to all relevant legal or industry standards or requirements;

f. obtain and maintain all necessary licenses and consents and comply with all applicable law in relation to the Services; and

g. timely perform the tasks designated as the responsibility of Client in the applicable SOW to facilitate CP Cyber's performance of the Services.

If CP Cyber's performance of its obligations under this Agreement is prevented or delayed by any act or omission of Client or its agents, subcontractors, consultants, or employees CP Cyber shall not be deemed in breach of its obligations under this Agreement or otherwise liable for any costs, charges, or losses sustained or incurred by Client.

2. Security Acknowledgement. Client acknowledges and agrees that no information security assessment can ever provide total assurance against potential security intrusions. The effectiveness of controls and security measures is subject to inherent limitations and all errors or problems may not be detected. Assessment results are subject to the risk that changes are made to Client's systems or controls, changes are made in processing requirements, changes are required because of the passage of time, or new technology is developed. CP Cyber is not responsible for any lack of specific controls, breach of security, or other errors or fraud related to any part of Client's systems.

Client is advised of the specific items and actions that CP Cyber has taken, is taking, and will take hereunder, and Client assumes all liability under applicable law, including without limitation, HIPAA privacy, and employment laws, which may arise from the access, services, or any other act undertaken by CP Cyber hereunder. Client shall maintain appropriate levels of insurance to cover its business including, without limitation, cybersecurity insurance.

If Client requests, or CP Cyber is required by court order or government regulation, subpoena, or other legal process, to produce document or personnel in connection with any proceeding, Client shall pay CP Cyber on a time and materials basis at then current rates for all fees and expenses incurred by CP Cyber in responding to such requests.

3. Advice and Recommendations. CP Cyber may provide advice and recommendations to assist Client's management personnel in making decisions but CP Cyber will not provide management functions or make management decisions on Client's behalf. CP Cyber is not liable for the actions or inactions of Client's management as it relates to Client's general business operations or CP Cyber's advice and recommendations.

4. Lost Time. If the applicable SOW indicates a fixed fee basis for payments then this Section shall apply. Any costs and expenses incurred by CP Cyber arising from Client's failure to provide timely responses and cooperation ("**Lost Time**") shall be the responsibility of Client and Client shall pay for all Lost Time at CP Cyber's then current time and materials rates, as CP Cyber shall provide and update from time to time. Any payments for Lost Time will be in addition to fixed fee payments owed under the applicable SOW. For purposes of this Agreement, "Lost Time" will include without limitation: (i) any time CP Cyber stands idle as a result of any failure of Client to perform Client's responsibilities as set forth in

the applicable SOW, and (ii) any time and materials expended by CP Cyber in an attempt to correct discrepancies in Services that are CP Cyber can establish arise from an error or discrepancy in materials, technology, or information provided by Client.

5. Failure of Assumptions. If the assumptions contained in a SOW on a fixed-fee basis fail, such that CP Cyber can meet milestones only through the expenditure of resources in excess of those contemplated by the parties, the parties shall in good faith execute a writing ("**Change Order**") stating, at a minimum: (i) the effective date of the Change Order; (ii) the specific changes, with reference to the affected sections of the SOW; and (iii) the effect of the changes on any fees or other amounts to be paid under the SOW. Once executed, a Change Order will become a part of, and will be incorporated into, the related SOW. If the parties are unable to reach agreement on such Change Order, CP Cyber may, in its discretion, terminate the related SOW and Client shall pay CP Cyber the fees for any Services performed before the effective date of termination, on a time and materials basis.

6. Client Acceptance of Work. At the conclusion of each SOW, CP Cyber and Client shall review the intended scope of work and deliverables to confirm CP Cyber has met the defined project expectations. If Client believe the deliverables do not conform, Client shall notify CP Cyber in writing within ten (10) days of receiving the deliverables that they do not conform. CP Cyber will then have a reasonable period of time, based upon the severity and complexity of the issue, to begin to correct the nonconformity and diligently pursue the same to completion. If you use the deliverables before acceptance, or if you fail to notify us of the nonconformance within the ten (10) day period, the deliverables will be considered accepted.

7. Loss of Data; System Downtime. Client understands and agrees that the Services, including installation or repair of components to any system, may cause data or software programs to be damaged, destroyed, or lost, whether it is a direct result or indirect result of any work performed on any systems within the environment during or after the Services are completed. Client also understands and agrees that Client is responsible for backing up all data and software programs in any system before any work is set to commence and that CP Cyber is not responsible for loss of data, programs, or loss of use of systems or networks arising out of the Services.

8. Authorization to Maintain and Access Client Devices. Client acknowledges that as a function of performing the Services, CP Cyber may access, connect to, and manage Client devices via remote technologies without first notifying Client (except where prohibited by law). These activities include, without limitation, updating or changing software drivers, installing and applying software patches, rebooting devices within maintenance windows, deleting temporary files and clearing caches, starting or restarting application services, staging and executing scripts for automated maintenance routines, network performance tuning, transferring data associated with routine system tuning and upkeep between systems, and identifying, collecting, and reporting on detailed data for devices on a network. Notwithstanding the above, Client is responsible for notifying CP Cyber of a restriction of remote access, connections or management activities related to any Client device.

9. Access. Client agrees and acknowledges that (a) in order to utilize some Services or portions thereof or access its data, applications, devices and network (collectively, the "**Resources**"), Client may be required to first download, or to permit to be downloaded, firmware, plug-ins, and software identified by CP Cyber and all updates, patches, and bug fixes thereto ("**Software**"); (b) any device onto which such Software cannot be downloaded, or does not otherwise function properly, may be unable to utilize some or all of the Services or access some or all of the Resources; (c) downloading and installing any Software will require system memory and disk space and may negatively impact the processing speed of Client's devices; (d) it will not reproduce, modify, distribute, publicly display, or reverse engineer, decompile or otherwise attempt to discover the source code for the Software in violation of the licensor's intellectual property rights; and

(e) changes to any other software, hardware, or the combination thereof associated may render partially or fully unavailable the Services that were previously available.

10. Third-Party Warranties. The Services may require CP Cyber to access devices or software that are not manufactured by CP Cyber. Some manufacturers' warranties may become void if CP Cyber or anyone else other than the manufacturer services these devices or software. It is Client's responsibility to ensure that CP Cyber's performance of Services will not affect such warranties or, if it does, that the effect will be acceptable to Client. CP Cyber is not responsible for third party warranties or for any effect that the Services may have on such warranties.

11. Term and Termination.

a. Term. The term of the Agreement commences on the Effective Date and continues for a period of one (1) year unless earlier terminated in accordance with Section 11(b) and (c) (the "**Initial Term**"). Following the Initial Term, the Agreement automatically renews for additional, successive periods of one (1) year unless earlier terminated in accordance with Section 11(b) and (c) (each a "**Renewal Term**" and together with the Initial Term, the "**Term**").

b. Termination for Convenience. Either party may terminate this Agreement, effective as of the end of the then current Initial Term or Renewal Term, by providing written notice to the other party at least thirty (30) days prior to the end of the then current Initial Term or Renewal Term.

c. Termination for Cause. Either party may terminate this Agreement or any SOW immediately upon written notice to the other party if the other party (i) refuses to or is unable to perform its obligations under the Agreement, (ii) breaches any part of the Agreement, (iii) files for bankruptcy, becomes or is declared insolvent, or is the subject of proceedings relating to its liquidation, insolvency, or appointment of a receiver, or (iv) makes an assignment for the benefit of its creditors. If CP Cyber terminates the Agreement in accordance with this Section 11(c), Client shall pay CP Cyber all fees for any Services performed through the date of termination on a time and materials basis at then current rates and all expenses and costs incurred by CP Cyber in performing the Services prior to the date of termination.

12. Representations and Warranties. Each party represents and warrants to the other party that:

a. it is duly organized, validly existing and in good standing as a corporation or other entity as represented herein under the laws and regulations of its jurisdiction of incorporation, organization, or chartering;

b. it has the full right, power, and authority to enter into this Agreement, to grant the rights and licenses granted hereunder, and to perform its obligations hereunder;

c. the execution of this Agreement by its representative whose signature is set forth at the end hereof has been duly authorized by all necessary corporate action of the party; and

d. when executed and delivered by such party, this Agreement will constitute the legal, valid, and binding obligation of such party, enforceable against such party in accordance with its terms.

13. Confidentiality.

a. Definition. "**Confidential Information**" means any information: (a) disclosed by one party (the "**Disclosing Party**") to the other (the "**Receiving Party**"), which, if in written, graphic, machine-readable, or other tangible form is marked as "Confidential" or "Proprietary," or which, if disclosed orally or by demonstration, is identified at the time of initial disclosure as confidential and reduced to writing and marked "Confidential" within thirty (30) days of such disclosure; (b) which is otherwise deemed to be confidential by the terms of this Agreement; or (c) which should be reasonably understood by the Receiving

Party to be the confidential or proprietary information of the Disclosing Party. By example, and without limitation, Confidential Information includes any and all non-public information that relates to the actual or anticipated business and/or products, research or development of the Disclosing Party, or to the Disclosing Party's technical data, trade secrets, or know-how, including, but not limited to, research, product plans, or other information regarding the Disclosing Party's products or services and markets therefor, customer lists and customers, software, developments, inventions, processes, formulas, technology, designs, drawings, engineering, hardware and network configuration information, network systems information, marketing, finances, and other business information disclosed by the Disclosing Party either directly or indirectly in writing, orally, or by drawings or inspection of premises, parts, equipment, or other Disclosing Party property.

b. Non-Use and Non-Disclosure. The Receiving Party shall treat as confidential all of the Disclosing Party's Confidential Information and shall not use or disclose such Confidential Information except as expressly permitted under this Agreement. Without limiting the foregoing, the Receiving Party shall use at least the same degree of care that it uses to prevent the disclosure of its own Confidential Information of like importance, but in no event with less than reasonable care, to prevent the disclosure of the Disclosing Party's Confidential Information.

c. Exclusions. The obligations of this Section shall not apply to Confidential Information that the Receiving Party can demonstrate: (a) was independently developed by the Receiving Party without any use of the Disclosing Party's Confidential Information; (b) becomes known to the Receiving Party from a source other than the Disclosing Party without breach of any obligation to Disclosing Party with respect to such information; (c) was in the public domain at the time it was disclosed or becomes in the public domain through no act or omission of the Receiving Party; or (d) was rightfully known to the Receiving Party at the time of disclosure.

d. Confidentiality of Agreement. Each party agrees that the terms and conditions, but not the existence, of this Agreement shall be treated as the other's Confidential Information and that no reference to the terms and conditions of this Agreement or to activities pertaining thereto can be made in any form of public or commercial advertising without the prior written consent of the other party; provided, however, that each party may disclose the terms and conditions of this Agreement: (a) as required by any court or other governmental body; (b) as otherwise required by law; (c) to legal counsel of the parties; (d) in connection with the requirements of an initial public offering or securities filing; (e) in confidence, to accountants, banks, and financing sources and their advisors; (f) in confidence, in connection with the enforcement of this Agreement or rights under this Agreement; or (g) in confidence, in connection with a merger or acquisition or proposed merger or acquisition, or the like.

e. Remedies. Unauthorized use by the Receiving Party of the Disclosing Party's Confidential Information will diminish the value of such Confidential Information. Therefore, if a party breaches any of its obligations with respect to confidentiality or use of Confidential Information hereunder, the other party shall be entitled to seek equitable relief to protect its interest therein, including but not limited to injunctive relief without the necessity of posting bond or other security, as well as money damages.

f. Return of Confidential Information. Upon expiration or termination of this Agreement for any reason, each party shall deliver to the other party all of the other party's Confidential Information that such party may have in its possession or control or shall destroy all such Confidential Information and certify such destruction in a writing signed by an authorized officer of such party. Notwithstanding the foregoing, subject to the terms of this Agreement, the Receiving Party shall be entitled to retain one archival copy of such Confidential Information for purposes of determining its obligations under this Agreement. This Agreement is not intended to prevent CP Cyber from using any ideas, concepts, know-how, or

techniques related to the Services that are retained in the unaided memories of CP Cyber's personnel who have had access to Confidential Information disclosed hereunder.

14. Intellectual Property Rights; Ownership.

a. Except as set forth in Section 14(c) or otherwise provided in an applicable SOW, Client is, and shall be, the sole and exclusive owner of all right, title, and interest in and to the documents, work product, and other materials that are prepared by CP Cyber and delivered to Client for Client's ongoing use in connection with the Services ("**Deliverables**"), including all patents, trademarks, copyrights and other intellectual property rights therein ("**Intellectual Property Rights**"). CP Cyber agrees, that with respect to any Deliverables that may qualify as "work made for hire" as defined in 17 U.S.C. § 101, such Deliverables are hereby deemed a "work made for hire" for Client. To the extent that any of the Deliverables do not constitute a "work made for hire", CP Cyber hereby irrevocably assigns to Client, in each case without additional consideration, all right, title, and interest throughout the world in and to the Deliverables, including all Intellectual Property Rights therein.

b. Upon Client's reasonable request, CP Cyber shall promptly take such further actions, including execution and delivery of all appropriate instruments of conveyance, as may be necessary to assist Client to prosecute, register, perfect, or record its rights in or to any Deliverables.

c. CP Cyber and its licensors are, and shall remain, the sole and exclusive owners of all right, title, and interest in and to all documents, data, know-how, methodologies, software, and other materials, including computer programs, reports, and specifications, provided by or used by CP Cyber in connection with performing the Services, in each case developed or acquired by the CP Cyber prior to the commencement or independently of the Agreement (the "**Pre-Existing Materials**"), including all Intellectual Property Rights therein. CP Cyber hereby grants Client a limited license to use any Pre-Existing Materials to the extent incorporated in, combined with or otherwise necessary for the use of the Deliverables. All other rights in and to the Pre-Existing Materials are expressly reserved by CP Cyber.

15. Indemnity. Each party (as "**Indemnifying Party**") shall indemnify the other party and its respective officers, directors, managers, members, partners, affiliates, agents, contractors, and employees (collectively, "**Indemnified Party**") and hold them harmless from any and all liabilities, losses, damages, costs, obligations, and expenses of whatever kind including, without limitation, attorneys' fees and the cost of enforcing indemnification hereunder, incurred by Indemnified Party in any claim, action, cause of action, demand, lawsuit, arbitration, inquiry, audit, notice of violation, proceeding, litigation, citation, summons, subpoena, or investigation of any nature, civil, criminal, administrative, regulatory, or otherwise, whether at law, in equity, or otherwise by a third party arising from or related to:

a. Material breach or non-fulfillment of any representation and warranty set forth in this Agreement;

b. Any negligent or mor culpable act or omission of Indemnifying Party (including reckless or willful misconduct) in connection with the performance of its obligations under this Agreement; or

c. Any bodily injury, death of any person, or damage to real or tangible personal property caused by the negligent or more culpable acts or omissions of Indemnifying Party.

Notwithstanding anything to the contrary in this Agreement, Indemnifying Party is not obligated to indemnify, hold harmless, or defend Indemnified Party against any claim (whether direct or indirect) if such claim or corresponding Losses arise out of or result from Indemnified Party's:

a. negligence or more culpable act or omission (including recklessness or willful misconduct); or

b. bad faith failure to comply with any of its obligations set forth in this Agreement.

16. Infringement Remedy. If the Services, or any component thereof other than Client Materials or Third Party Materials, are found to be infringing or if any use of the Services or any component thereof is enjoined, threatened to be enjoined, or otherwise the subject of an infringement claim, CP Cyber shall, at its option and sole cost and expense: (a) procure for Client the right to continue to use the affected Services or component thereof to the full extent contemplated by this Agreement; or (b) modify or replace the materials that infringe or are alleged to infringe ("**Allegedly Infringing Materials**") to make the Services and all of their components non-infringing while providing fully equivalent features and functionality. If neither of the foregoing is possible notwithstanding CP Cyber's commercially reasonable efforts then CP Cyber may direct Client to cease any use of any materials that have been enjoined or finally adjudicated as infringing, provided that CP Cyber shall refund to Client all amounts paid by Client in respect of such Allegedly Infringing Materials. The foregoing is the sole remedy available to Client under this Agreement or otherwise with respect to infringement of the Services or a component thereof.

17. Non-Solicitation. During the Term and for a period of twelve (12) months thereafter, Client shall not, directly or indirectly, in any manner solicit or induce for employment any person who performed any work under the Agreement who is then in the employ of the other party. A general advertisement or notice of a job listing or opening or other similar general publication of a job search or availability to fill employment positions, including on the internet, shall not be construed as a solicitation or inducement for the purposes of this Section. If Client breaches this Section, Client shall, on demand, pay to CP Cyber a sum equal to the greater of $75,000 or one and one half (1.5) times one year's basic salary or the annual fee that was payable by CP Cyber to that employee, worker, or independent contractor.

18. Further Assurances. Each party shall, upon the reasonable request of the other party, execute such documents and perform such acts as may be necessary to give full effect to the terms of this Agreement.

19. Relationship of the Parties. The relationship between the parties is that of independent contractors. Nothing contained in this Agreement shall be construed as creating any agency, partnership, joint venture, or other form of joint enterprise, employment, or fiduciary relationship between the parties, and, except as expressly provided herein, neither party shall have authority to contract for or bind the other party in any manner whatsoever.

20. Governing Law. This Agreement shall be governed by and construed in accordance with the internal laws of Colorado without giving effect to any choice or conflict of law provision or rule.

21. Notice. All notices, requests, consents, claims, demands, waivers, and other communications hereunder shall be in writing and shall be deemed to have been given (a) when delivered by hand (with written confirmation of receipt); (b) when received by the addressee if sent by a nationally recognized overnight courier (receipt requested); (c) on the date sent by email if sent during normal business hours of the recipient, and on the next business day if sent after normal business hours of the recipient or (d) on the third day after the date mailed, by certified or registered mail, return receipt requested, postage prepaid. Such communications must be sent to the respective parties at the addresses indicated on the signature page of the Agreement (or at such other address for a party as shall be specified in a notice given in accordance with this Section).

22. Subcontractors. CP Cyber may, in its discretion, delegate certain obligations relating to the Services to third parties. Client shall have the benefit of all rights, remedies, and redress against such third parties that CP Cyber has under the applicable contract with such third party. CP Cyber shall provide a copy of such contracts to Client upon request and Client hereby acknowledges that CP Cyber shall not be liable for

the performance or failure of performance of such third parties and that Client shall pursue such third parties directly for any claims arising from the applicable Services.

23. No Liability for Third Parties. Performance of the Services may involve the use of third party software or tools as indicated in the applicable SOW or as otherwise determined by CP Cyber. Client hereby agrees to abide by the terms and conditions applicable to any third party software or tools used by CP Cyber in performing the Services. CP Cyber shall provide Client a copy of the applicable terms and conditions for third party software and tools in use upon request. CP Cyber hereby disclaims all warranties regarding such third party software and tools and shall not be liable for the acts or omissions of such third parties or for Client's breach of the applicable terms and conditions.

24. Assignment. Except as provided in Section 22, neither party may assign, transfer, or delegate any or all of its rights or obligations under this Agreement, without the prior written consent of the other party; provided, that, upon prior written notice to the other party, either party may assign the Agreement to an Affiliate of such party or to a successor of all or substantially all of the assets of such party through merger, reorganization, consolidation, or acquisition. No assignment shall relieve the assigning party of any of its obligations hereunder. Any attempted assignment, transfer, or other conveyance in violation of the foregoing shall be null and void. This Agreement shall be binding upon and shall inure to the benefit of the parties hereto and their respective successors and permitted assigns.

25. Amendment; Waiver. This Agreement may be amended, modified, or supplemented only by an agreement in writing signed by each party hereto. No waiver by any party of any of the provisions hereof shall be effective unless explicitly set forth in writing and signed by the party so waiving. Except as otherwise set forth in this Agreement, no failure to exercise, or delay in exercising, any rights, remedy, power, or privilege arising from this Agreement shall operate or be construed as a waiver thereof; nor shall any single or partial exercise of any right, remedy, power, or privilege hereunder preclude any other or further exercise thereof or the exercise of any other right, remedy, power, or privilege.

26. Severability. If any term or provision of this Agreement is invalid, illegal, or unenforceable in any jurisdiction, such invalidity, illegality, or unenforceability shall not affect any other term or provision of this Agreement or invalidate or render unenforceable such term or provision in any other jurisdiction. Upon such determination that any term or other provision is invalid, illegal, or unenforceable, the parties hereto shall negotiate in good faith to modify this Agreement so as to affect the original intent of the parties as closely as possible in a mutually acceptable manner in order that the transactions contemplated hereby be consummated as originally contemplated to the greatest extent possible.

27. Dispute Resolution. The parties shall resolve any dispute, controversy, or claim arising out of or relating to this Agreement, or the breach, termination, or invalidity hereof (each, a "**Dispute**"), under the provisions of this Section. The procedures set forth in this Section shall be the exclusive mechanism for resolving any Dispute that may arise from time to time and are express conditions precedent to litigation of the Dispute.

a. Negotiations. A party shall send written notice to the other party of any Dispute ("**Dispute Notice**"). The parties shall first attempt in good faith to resolve any Dispute set forth in the Dispute Notice by negotiation and consultation between themselves, including not fewer than two (2) negotiation sessions. In the event that such Dispute is not resolved on an informal basis within thirty (30) days after one party delivers the Dispute Notice to the other party, whether the negotiation sessions take place or not, either party may initiate mediation.

b. Mediation. After the period for negotiation, either party may submit the Dispute to any mutually agreed to mediation service for mediation by providing to the mediation service a joint, written

request for mediation, setting forth the subject of the dispute and the relief requested. The parties shall cooperate with one another in selecting a mediation service, and shall cooperate with the mediation service and with one another in selecting a neutral mediator and in scheduling the mediation proceedings. The parties covenant that they will use commercially reasonable efforts in participating in the mediation. The parties agree that the mediator's fees and expenses and the costs incidental to the mediation will be shared equally between the parties. The parties further agree that all offers, promises, conduct, and statements, whether oral or written, made in the course of the mediation by any of the parties, their agents, employees, experts, and attorneys, and by the mediator and any employees of the mediation service, are confidential, privileged, and inadmissible for any purpose, including impeachment, in any litigation, arbitration or other proceeding involving the parties, provided that evidence that is otherwise admissible or discoverable shall not be rendered inadmissible or non-discoverable as a result of its use in the mediation.

c. Litigation as a Final Resort. If the parties cannot resolve any Dispute for any reason, including, but not limited to, the failure of either party to agree to enter into mediation or agree to any settlement proposed by the mediator, within sixty (60) days after the start of mediation, either party may file suit in a court of competent jurisdiction. Any legal suit, action, or proceeding arising out of or related to this Agreement or the Services provided hereunder shall be instituted exclusively in the federal courts of the United States or the courts of Colorado in each case located in the city of Denver, and each party irrevocably submits to the exclusive jurisdiction of such courts in any such suit, action, or proceeding. Service of process, summons, notice, or other document by mail to such party's address set forth herein shall be effective service of process for any suit, action, or other proceeding brought in any such court.

28. Attorneys' Fees. If any party institutes any legal suit, action, or proceeding against the other party arising out of or related to this Agreement or any SOW, including but not limited to contract, equity, tort, fraud, and statutory claims, the substantially prevailing party in the suit, action or proceeding is entitled to receive, and the non-prevailing party shall pay, in addition to all other remedies to which the prevailing party may be entitled, the costs and expenses incurred by the prevailing party in conducting or defending the suit, action, or proceeding, including reasonable attorneys' fees and expenses and court costs, even if not recoverable by law.

29. Force Majeure. No party shall be liable or responsible to the other party, or be deemed to have defaulted under or breached this Agreement, for any failure or delay in fulfilling or performing any term of this Agreement (except for any obligations to make payments to the other party hereunder), when and to the extent such failure or delay is caused by or results from acts beyond the impacted party's ("**Impacted Party**") control, including without limitation the following force majeure events ("**Force Majeure Events**"): (a) acts of God; (b) flood, fire, earthquake, epidemic, or explosion; (c) war, invasion, hostilities (whether war is declared or not), terrorist threats or acts, riot, or other civil unrest; (d) government order, law, or actions; (e) embargoes or blockades in effect on or after the date of this Agreement; (f) national or regional emergency; and (g) other similar events. The Impacted Party shall give notice within five (5) days of the Force Majeure Event to the other party, stating the period of time the occurrence is expected to continue. The affected party shall use diligent efforts to end the failure or delay and ensure the effects of such Force Majeure Event are minimized and shall resume performance of its obligations as soon as reasonably practicable after the removal of the cause.

30. Order of Precedence. If there is any conflict between the terms of these Standard Terms, the terms of the Strategic Cybersecurity Services Master Services Agreement between CP Cyber and the applicable client, and the terms of any applicable SOW the following order of precedence shall apply: first the terms of any applicable SOW, second the terms of the Strategic Cybersecurity Services Master Services Agreement or SOW between CP Cyber and the applicable client, and third, terms of these Standard Terms.

Service Level Agreement (SLA)

For Managed Security Services

---

1. Purpose

This SLA defines the services, performance metrics, responsibilities, and expectations agreed upon by the Client and Cornerstone Partners, LLC (CP Cyber or MSSP) for managed security services.

---

2. Scope of Services

The MSSP will provide the following services:

- **Endpoint Protection (EDR/XDR/AV)–** Malicious files, scripts, log data, remote access, hacker utilities, local network traffic protection, local DNS protection.
- **24/7/365 End Point Monitoring** – CP Cyber's dedicated team continuously monitors security events from our end point security tools.
- **Incident Analysis and Triage** – CP Cyber's experts will analyze security incidents, conduct initial triage and escalate incidents.
- **Real-Time Alerts:** CP Cyber will provide real-time notifications of suspicious activity.
- **Response:** CP Cyber's managed cloud suite will proactively alert and block user cloud accounts with known malicious behavior to prevent a malicious actor from gaining unauthorized access.
- **Log collection, aggregation, and analysis (SIEM):** CP Cyber captures, stores, and analyzes the logs . Analysis is performed with defined Threat Hunting procedures.

---

3. Service Hours

Service Component	Availability
SOC Monitoring	24/7/365
Incident Response	24/7/365
Client Support / Helpdesk	9 AM – 5 PM MST (Mon–Fri) excluding company holidays
Emergency Support	24/7/365 via escalation process

---

4. Performance Metrics

Metric	Target Level
Incident Response Initiation	< 30 minutes for Critical; < 2 hours for High; < 8 business hours for Medium
Ticket Acknowledgement Time	< 30 minutes
Mean Time to Resolution (MTTR)	< 4 hours (Critical), < 24 hours (High)

5. Incident Severity Classification

Severity Level	Description
Critical	Severe security breach or system compromise
High	Elevated threat, not a critical impact
Medium	Suspicious threat
Low	Informational or non-urgent item

6. Client Responsibilities

- Provide timely access to systems, logs, and personnel
- Maintain up-to-date contact information for escalation
- Implement recommendations from MSSP in a timely manner
- Participate in regular security reviews and meetings

Client-side delays can directly impact SLA adherence. For example, slow approvals, long response times, or restricted access may hinder incident resolution and stretch timelines beyond agreed thresholds.

7. Review and Governance

- **Service Review Meetings:** Monthly or as agreed
- **Escalation Path:** Provided in Appendix A

---

8. Penalties and Remedies

If the MSSP fails to meet agreed-upon service levels:

- **Service Credits**: 1% of monthly fee per SLA breach (cap: 10%)
- **Termination Right**: Continued and Repeated SLA breaches over 3 months may lead to contract termination

Client-side delays can directly impact SLA adherence and therefore, Cornerstone Partners, LLC will not be liable or responsible for unmet SLA's where slow communication, approvals or restricted access by Client hinder incident resolution and stretch timelines beyond agreed thresholds.

---

9. Change Management

Changes to the SLA or service scope will follow a formal **Change Request Process**, documented and approved by both parties.

Appendix A – Escalation Matrix

Priority Level	Communication Method	Client Engagement
Critical	Ticket + Phone Call	Immediate outreach to Client POC for acknowledgement and action
High	- If active incident: Follow **Critical** process - If not active: Email Alert + Follow-up (phone, email, text as needed)	Ensure client is informed and remediation steps are acknowledged
Medium	Email Alert + Best-effort follow-up via email	Monitor for response, escalate if no action taken or risk increases
Low	Automatic Email Alerts	No immediate follow-up unless requested by client or issue escalates

Appendix B – Definitions

Key Terms in a Managed Security Service Provider (MSSP) Environment

---

Monitoring & Detection

SIEM (Security Information and Event Management)
A platform that aggregates and analyzes logs and events from various sources across an IT environment. SIEMs enable real-time threat detection, incident correlation, and compliance reporting.

SOC (Security Operations Center)
A centralized team and technology stack responsible for 24/7 monitoring, detection, investigation, and response to cybersecurity incidents.

Endpoint & Extended Detection

AV (Antivirus)
A traditional security solution that scans files and programs on endpoints (like desktops or servers) for known malware based on signature detection. While AV can stop many common threats, it often lacks visibility into more advanced or evasive attacks.

EDR (Endpoint Detection and Response)
A more advanced endpoint security solution that goes beyond antivirus. EDR continuously monitors endpoint activity, detects suspicious behavior, and provides detailed visibility for investigation and response. It enables analysts to isolate hosts, kill processes, and contain threats in real time.

XDR (Extended Detection and Response)
An evolution of EDR that unifies threat detection and response across multiple data sources — not just endpoints, but also network traffic, email, cloud workloads, and identity platforms. XDR provides a centralized view of threats across the environment and helps correlate signals to reduce alert fatigue and improve response accuracy.

Events, Incidents & Response

Event
Any observable occurrence in a system or network. Not all events are malicious — examples include logins, system updates, or configuration changes.

Incident
An event — or series of related events — that threaten the confidentiality, integrity, or availability of information assets. Incidents typically require investigation and response. Examples include malware infections, unauthorized access, or data exfiltration.

Critical Incident
A high-severity incident with the potential to cause major disruption to business operations, data, or infrastructure. These incidents require immediate attention and may trigger escalation procedures.

Response Metrics & Client Impact

Response Time
The amount of time between the detection or reporting of a security event and the first action taken by the MSSP (such as triage or investigation).

Client responsiveness directly affects response time. Delayed acknowledgments, missing context, or access restrictions can all slow down our ability to act.

MTTR (Mean Time to Respond/Resolve)
The average time taken to fully detect, investigate, contain, and resolve a security incident.

MTTR is a shared metric. While MSSP teams aim to act quickly, delays in client-side communication, approvals, or follow-up actions can significantly extend resolution time and cause the required MTTR's to not be met. Cornerstone Partners, LLC is not liable for or responsible for unmet MTTR's due to delays or lack of client communication, approvals, or follow-up actions.

False Positive
An alert that initially appears to indicate a threat but is determined to be benign after investigation. Minimizing false positives is key to reducing noise and improving analyst focus.

Threat Intelligence & Risk

IOCs (Indicators of Compromise)
Artifacts or clues that suggest a system may have been breached. Examples include suspicious IP addresses, file hashes, or domain names linked to malware.

TTPs (Tactics, Techniques, and Procedures)
Patterns of behavior used by threat actors. Understanding TTPs helps in proactive threat hunting and detection rule creation.

Risk Assessment
The process of identifying and evaluating potential threats, vulnerabilities, and the impact of different risks on business operations or IT assets.