SOLCYBER MANAGED SECURITY SERVICES, INC.

SOLCYBER TERMS OF SERVICE

SolCyber Managed Security Services, Inc., a Delaware corporation with offices located at 1920 McKInney Ave., Suite 700, Dallas, TX 75201 (”SolCyber”) and provides the Services (as defined below) to the customer (”**Customer**”) executing an order form with SolCyber. These Terms of Service (the "Terms of Service") contain the terms and conditions that govern the use of all SolCyber Services, which shall be ordered from SolCyber through order forms subject to these Terms of Service. SolCyber and Customer may be referred to herein collectively as the "**Parties**” or individually as a ”Party.”

1 Definitions

(a) *”Authorized Site”* means a web portal through which Authorized Users may access the Software.

(b) *”Authorized User”* means an employee, consultant, or independent contractor of Customer, and identified by Customer as such, who i) has received a valid password and login ID from SolCyber or from Customer’s User Administrator (see Section 3 below) to access the Software or Services and ii) has accepted and agreed to the terms of these Terms of Service.

(c) ”Customer Data” means all electronic information provided by Customer to SolCyber under these Terms of Service (including, without limitation, employee information, Customer information, application configurations, and data related to Customer security and reporting).

(d) *”Customization”* means a specific software-based Deliverable that includes new code or an adaptation (e.g., a change to source code) to the base Software and/or product embedded customized objects, which Deliverable has been furnished as part of a Statement of Work (including, without limitation, custom applications integrations, custom reports, and or on-boarding procedures). For the avoidance of doubt, configuration of the base Software is not a Customization.

(e) *”Deliverables”* means any tangible and intangible materials, including reports, studies, base cases, drawings, findings, manuals, procedures and recommendations that are prepared by SolCyber for Customer pursuant to a Statement of Work in the course of furnishing the Software and Documentation.

(f) *”Documentation”* means the standard SolCyber help materials, user documentation, and training materials normally made available by SolCyber in connection with specific Software products.

(g) *"Incident Response Services"* means the Incident response services procured through SolCyber's third party service provider and subcontractor, Surefire Cyber, Inc. ("Surefire").

(h) *"Managed Security Services"* means the cybersecurity, managed security, monitoring, security operations center (SOC), and/or similar services that may be performed on a subscription or recurring basis as set forth in a Statement of Work.

(i) *"Modification"* means a modification, alteration, addition, derivative work, derivation, enhancement and/or improvement of any kind to or of or from or based on or related to the Deliverable, and/or any part thereof, in any form or format. For the avoidance of doubt, configuration of the base Software is not a Modification.

(j) *"Professional Services"* means the services to be performed by SolCyber for Customer (excluding Software or Managed Security Services) in accordance with Section 4 herein and as further detailed in a Statement of Work.

(k) *"Software"* means the services to be performed by SolCyber for Customer (excluding Software, Managed Security Services, or Incident Response Services) in accordance with Section 4 herein and as further detailed in a Statement of Work.

(l) *"Statement of Work"* (also referred to as an "SOW") means a document in writing signed or accepted by both Parties, that: (a) details the scope of work of the Managed Security Services, Professional Services, or Incident Response Services to be performed by SolCyber under these Terms of Service, including identification of Deliverables and other materials to be provided to Customer, if any; (b) identifies the locations at which the Managed Security Services, Professional Services, or Incident Response Services shall be performed; and (c) specifies the applicable payment terms, including the hourly rate or unit rates, for performing the Managed Security Services, Professional Services, or Incident Response Services.

(m) *"Term"* means the period of time these Terms of Service are in effect, including the initial term and any extensions or renewals thereof.

(n) *"Update"* means any updates, bug fixes, patches, maintenance releases, or other error corrections to the Software that SolCyber generally makes available free of charge to all customers of the Software.

2 Services and Limited Licenses.

(a) <u>Services.</u> The term "Services" in these Terms of Service means, collectively, the Managed Security Services, Professional Services, including any Software that may be included as part of the provision of the foregoing, and Incident Response Services, as identified in a Statement of Work or detailed in an applicable Statement of Work. SolCyber may use one or more affiliated entities and/or subcontractors to provide the Services in accordance with these Terms of Service.

(b) <u>License to Customer. To enable Customer to use the Services, SolCyber grants to Customer, during the Term, a personal, limited, non-exclusive, non-sublicensable, non-transferable and non-assignable license (except in compliance with Section 14(a)) for Authorized Users solely to</u>

(i) access and execute the Software through the Authorized Site and use the applicable Documentation strictly for the benefit of Customer's internal business operations and (ii) input and upload Customer Data in connection with the operation of the Software under these Terms of Service.

(c) License to SolCyber. To enable SolCyber to provide the Services, Customer grants to SolCyber, during the Term, a personal, non-exclusive, non-sublicensable license to use, reproduce, transmit and modify the Customer Data solely in connection with SolCyber provision of the Services, which for the avoidance of doubt includes SolCyber's testing, monitoring, reporting, modeling, and benchmarking of the Software and use thereof.

3 Customer Obligations

(a) Security & Infrastructure Obligations. Customer will be responsible for designating an employee or other person ("User Administrator") who shall be responsible for i) notifying SolCyber of each Authorized User for which it wishes to have access to the Software or Services; ii) identifying the roles and rights of each Authorized User; and iii) facilitating Customer's review of usage logs and other auditing or reporting information provided by SolCyber. Customer will be responsible for maintaining the confidentiality and security of such passwords and login IDs and all activities that occur under these IDs, regardless of whether such passwords and login IDs are generated and managed by Customer or by SolCyber. Customer will ensure that each login ID and password issued to an Authorized User will be used only by that Authorized User. Customer agrees to notify SolCyber promptly of any actual or suspected unauthorized use of any account, login ID or passwords, or any other breach or suspected breach of these security requirements. SolCyber reserves the right to suspend or terminate any login ID which SolCyber reasonably believes may have been used by an unauthorized third party or by any user or individual other than the Authorized User to whom such login ID and password was rightfully assigned. Customer is also responsible for maintaining the required hardware, software, Internet connections and other resources necessary for Customer and Authorized Users to access the Software through the Authorized Site.

(b) Other Customer Responsibilities. During the term of these Terms of Service, Customer will provide SolCyber with reasonable access to requested resources such as (i) information about Customer personnel, facilities, equipment, hardware, software, network and information, and (ii) timely decision-making, notification of relevant issues or information, identification of bugs in Software, and granting of approvals or permissions as reasonably necessary for SolCyber to provide the Software and/or Services under these Terms of Service. SolCyber shall not be responsible for any delay or other consequences resulting from Customer's failure to perform any of its obligations hereunder. Customer's failure to satisfy its responsibilities may lead to an increase in SolCyber's fees, depending on the extent to which SolCyber has to provide additional effort or reschedule its commitments to deliver the Software and/or Services, or SolCyber's inability to provide the Software and/or Services.

4 Professional Security, Managed Security, or Incident Response Services.

(a) Scope of Service. SolCyber shall perform the Services set forth and as detailed in any mutually agreed or accepted Statement of Work. If the Parties desire changes to the Services, including alterations in, additions to, or deletions from the Services, or changes in the sequence of the performance of the Services, and such request affects the completion, substance, and/or fees, as defined therein, the change shall be mutually agreed to in writing. SolCyber shall perform all Services in a professional, workmanlike, and diligent manner using appropriately skilled, qualified, professional, and competent personnel.

(b) Customizations. SolCyber shall perform Customizations as set out in any agreed Statement of Work, in which case Customer will have the same license usage rights to the Customizations as it has to the Software licensed hereunder.

5 Ownership & Proprietary Rights.

(a) SolCyber Intellectual Property. SolCyber owns or is an authorized licensee for all intellectual property used for purposes of providing the Services under these Terms of Service, whether developed prior to the commencement of these Terms of Service or anytime thereafter (the "SolCyber Properties"). All right, title, and interest in and to the SolCyber Properties (including, without limitation, all copyright, patent, trade secret, trademark and other intellectual property rights) and any Customizations, corrections, updates, adaptations, enhancements, improvements, translations or copies of the foregoing shall remain or vest exclusively with SolCyber.

(b) Customer Intellectual Property. All right, title, and interest in and to the Customer Data shall be owned exclusively by Customer, provided that Customer grants to SolCyber a non-exclusive, worldwide license to copy, transmit, modify and use the Customer Data solely for purposes of providing the Services.

(c) Deliverables. Except as otherwise set forth in these Terms of Service, the Deliverables created specifically for Customer by SolCyber are considered "works made for hire" and upon payment of all fees and expenses due for the Services, such Deliverables shall be owned exclusively by the Customer. To the extent that such Deliverables are determined not to constitute "works made for hire" as a matter of law, SolCyber hereby irrevocably assigns and transfers such property, and all right, title and interest therein, including all intellectual property rights, to the Customer and its successors and assigns. Notwithstanding the foregoing, "works made for hire" and the Deliverables shall not include SolCyber's preexisting information and methodologies for delivery of the Services or Software, document templates, working papers, Confidential Information (as defined below) or project tools used by SolCyber to perform the Services.

6 Confidential Information.

From time to time during the Term, either Party may disclose or make available to the other Party information about its business affairs, products, confidential intellectual property, trade secrets, third-party confidential information, and other sensitive or proprietary information, whether orally or in written, electronic, or other form or media, and whether or not marked, designated, or otherwise identified as "confidential" (collectively, "**Confidential Information**"). Without limiting the foregoing, the Services, Customer Data, and terms of these Terms of Service shall be considered Confidential Information. Confidential Information does not include information that the receiving Party can demonstrate that, at the time of disclosure is: (a) in the public domain; (b) known to the receiving Party; (c) rightfully obtained by the receiving Party on a non-confidential basis from a third party; or (d) independently developed by the receiving Party. The receiving Party shall not disclose the disclosing Party's Confidential Information to any person or entity, except to the receiving Party's employees, agents, contractors, consultants and representatives, including its bankers, attorneys and accountants (collectively "**Representatives**") who have a need to know the Confidential Information for the receiving Party to exercise its rights or perform its obligations hereunder, and then only under a written confidentiality agreement or other binding confidentiality obligation no less restrictive than this Section 6. The receiving Party on behalf of itself and its Representatives agrees that it will treat Confidential Information of the disclosing Party with the same degree of care as it accords to its own confidential information of like sensitivity, but in no event less than a reasonable level of care. The receiving Party further ensures that it and its Representatives will use the disclosing Party's Confidential Information only for the purposes contemplated by these Terms of Service. Notwithstanding the foregoing, each Party may disclose Confidential Information to the limited extent required (i) in order to comply with the order of a court or other governmental body, or as otherwise necessary to comply with applicable law, provided that the Party making the disclosure pursuant to the order shall first have given written notice to the other Party and made a reasonable effort to obtain a protective order; or (ii) to establish a Party's rights under these Terms of Service, including to make required court filings. On the expiration or termination of the Terms of Service, the receiving Party shall promptly return, subject to the provisions In Section 12 (c), to the disclosing Party all copies, whether in written, electronic, or other form or media, of the disclosing Party's Confidential Information, or destroy all such copies and certify in writing to the disclosing Party that such Confidential Information has been destroyed.

7 Restrictions.

Customer shall not sell, rent, lease, sublicense, distribute, transfer, copy, reproduce, download, display, generate any Modification, timeshare, or otherwise exploit in any other manner the Software or use such as a component of or a base for products or services prepared for commercial sale, sublicense, lease, access or distribution. Customer shall not itself, or cause or permit any Authorized User to, translate, reverse engineer, decompile, disassemble the Software or attempt to obtain in any other manner any Software source code. Customer shall not cause or allow any third party or unlicensed user or computer system, other than an Authorized User, to access or use the Software. Customer shall not introduce any infringing or otherwise unlawful data or material or any virus, spyware, malware or disabling code into the Software or into SolCyber systems or environment or attempt to deactivate or evade any protection mechanism of the Software, nor shall Customer remove, obscure or alter any intellectual property right or confidentiality notices or legends appearing in or on any aspect of the Software. Customer will not use SolCyber Properties to develop competitive products or services.

8 Warranties and Warranty Disclaimers.

(a) SolCyber Warranties. SolCyber will perform the Professional Services and Managed Security Services in a professional, workmanlike, and diligent manner, using appropriately skilled, qualified, professional and competent personnel.

(b) SolCyber Warranties Disclaimer. EXCEPT FOR THE WARRANTIES SET FORTH IN SECTIONS 8(a) and 8(c), ALL SOLCYBER PROPERTIES ARE PROVIDED ”AS IS.” SOLCYBER DOES NOT WARRANT THAT THE SOFTWARE OR SERVICES WILL MEET END USER’S REQUIREMENTS, THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT ALL DEFECTS IN THE SOFTWARE WILL BE CORRECTED. TO THE FULL EXTENT PERMITTED BY LAW, SOLCYBER AND IT’S AFFILIATES, EMPLOYEES, OFFICERS, DIRECTORS, AGENTS, AND LICENSORS, DISCLAIMS ALL OTHER WARRANTIES WHETHER EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF ANY INTELLECTUAL PROPERTY RIGHTS. FURTHER, SOLCYBER SHALL NOT BE LIABLE FOR ANY BUSINESS DECISIONS MADE OR IMPLEMENTED BY END USER BASED ON END USER’S USE OF THE SERVICES.

(c) Mutual Warranties. Each Party represents, warrants, and covenants that (i) it is a business entity duly organized and in good standing in all jurisdictions where it does business; (ii) has the full power and authority to enter into and perform its obligations under these Terms of Service; (iii) it will comply with all applicable laws in connection with its performance hereunder, including all export control laws.

9 Limitations of Liability.

EXCEPT FOR BREACHES OF SECTIONS 2, 3, OR 6, NEITHER PARTY SHALL BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, PUNITIVE, OR EXEMPLARY LOSSES, DAMAGES, EXPENSES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR DATA USE, OR OTHER PECUNIARY LOSS, WHETHER IN AN ACTION IN CONTRACT OR TORT INCLUDING NEGLIGENCE, ARISING OUT OF OR IN ANY WAY RELATED TO THIS AGREEMENT, THE PERFORMANCE HEREOF, THE USE OF SOFTWARE, SERVICES OR DELIVERABLES PROVIDED HEREUNDER, AND SUCH ALLEGED PARTY'S BREACH OF THIS AGREEMENT EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. EACH PARTY'S LIABILITY FOR DAMAGES HEREUNDER SHALL IN NO EVENT EXCEED IN THE AGGREGATE OF THE AMOUNT OF FEES PAID AND OWED BY END USER UNDER THIS AGREEMENT FOR THE IMMEDIATELY PRECEEDING TWELVE (12) MONTH PERIOD, EXCEPT TO THE EXTENT SUCH LIABILITY IS FINALLY JUDICIALLY DETERMINED TO HAVE RESULTED FROM A PARTY'S GROSS NEGLIGENCE, FRAUD, OR WILLFUL MISCONDUCT, IN WHICH CASE THE LIMITS HEREIN WILL NOT APPLY. THE PARTIES HAVE AGREED THAT THESE LIMITATIONS WILL SURVIVE AND APPLY EVEN IF ANY LIMITED REMEDY SPECIFIED IN THIS AGREEMENT IS FOUND TO HAVE FAILED OF ITS ESSENTIAL PURPOSE. THE LIMITATIONS OF LIABILITY CONTAINED IN THE AGREEMENT WILL APPLY ONLY TO THE MAXIMUM EXTENT PERMISSIBLE UNDER APPLICABLE LAW, AND NOTHING IN THE AGREEMENT PURPORTS TO LIMIT EITHER PARTY'S LIABILITY IN A MANNER THAT WOULD BE UNENFORCEABLE OR VOID AS AGAINST PUBLIC POLICY IN THE APPLICABLE JURISDICTION.

10 Indemnification.

(a) SolCyber Indemnification. SolCyber, at its expense, shall defend, indemnify and hold Customer harmless from and against any loss, damages, liability, or expenses (including, but not limited to, reasonable attorneys' fees and expenses) or liability from any claim, suit or proceeding (collectively, a "**Claim**"), to the extent arising out of, or related to, (i) the use by Customer of the Software in strict accordance with these Terms of Service and alleging infringement of a United States patent or a copyright or trade secret right of any third party; or (ii) SolCyber's gross negligence or willful misconduct; provided that Customer: (1) promptly notifies SolCyber of such Claim; (2) provides SolCyber with full control of the defense and settlement of each such Claim; (3) cooperates with SolCyber in such defense and settlement, and (4) does not settle any such Claim or suit without SolCyber's prior written consent. Customer may participate in the defense and settlement of any Claim with counsel of its choice at its own expense provided that SolCyber shall continue to have sole control of such defense or settlement. If any portion of the Software becomes, or in SolCyber's opinion is likely to become, the subject of a claim of infringement, SolCyber may, at its option: (A) procure for Customer the right to continue using the Software; (B) replace the Software with non-infringing services which do not materially impair the functionality of the Software; (C) modify the Software so that it becomes non-infringing; or (D) terminate these Terms of Service and refund any unused fees actually paid by Customer to SolCyber for the remainder of the term then in effect, and upon such termination, Customer will immediately cease all use of the Software. Notwithstanding the foregoing, SolCyber shall have no obligation under this section or otherwise with respect to any infringement claim based upon (I) any use of the Software not in accordance with these Terms of Service or not as specified in the Documentation; (II) any use of the Software in combination with other products, equipment, software or data not supplied by SolCyber if the Software without such combination does not infringe; (III) any modification of the Software by any person other than SolCyber or its authorized agents; (IV) a superseded Software version if a corrective Update has been made available to Customer; or (V) a Customization to the extent based on Customer-supplied intellectual property, materials, specifications, or information. This Section 10(a) states the sole and exclusive remedy of Customer and the entire liability of SolCyber with respect to infringement claims and actions.

(b) Customer Indemnification. Customer, at its expense, shall defend, indemnify, and hold SolCyber harmless for any Claims to the extent arising out of, or related to: (i) Customer's use of the Software, Services, or Deliverables in breach of these Terms of Service or in violation of any applicable laws, regulations, or ordinances; (ii) SolCyber's use of the Customer Data; (iii) any Modification to a Deliverable not made by or at the direction of SolCyber; or (iv) Customer's gross negligence or willful misconduct, provided that SolCyber: (1) promptly notifies Customer of such Claims; (2) provides Customer with full control of the defense and settlement of each such Claim; (3) cooperates with Customer in such defense and settlement, and (4) does not settle any such Claim without Customer's prior written consent. SolCyber may participate in the defense and settlement of any Claim with counsel of its choice at its own expense provided that Customer shall continue to have sole control of such defense or settlement.

11 Fees.

Customer shall pay SolCyber the Services fees in the amount and according to the schedule set forth in the applicable Order Form or Statement of Work. Unless otherwise provided in the applicable order form, Customer shall pay the Services fees and/or expenses within thirty (30) days from the invoice date. Customer shall be responsible for all sales, use and value added taxes, withholdings and any other taxes and charges of any kind imposed by any federal, state or local governmental or international entity on the transactions contemplated by these Terms of Service (collectively "Transactional Taxes"), excluding only federal, state and local taxes determined based on SolCyber's net income, such that the fees invoiced are exclusive of Transactional Taxes; shall be borne exclusively by the Customer; and shall not be considered a part of, a deduction from or an offset against such fees. All invoice payments due to SolCyber shall be made without any deduction or withholding on account of any Transactional Taxes, duty, charge or penalty except as required by law in which case the sum payable by Customer in respect of which such deduction or withholding is to be made shall be increased to the extent necessary to ensure that, after making such deduction or withholding, SolCyber receives and retains (free from any liability in respect thereof) a net sum equal to the sum it would have received but for such deduction or withholding being required.

12 Term & Termination.

(a) Term. These Terms of Service shall commence upon execution of an order form incorporating these terms and will continue for as long as any order forms incorporating these Terms of Service are in effect unless and until either Party gives notice of termination in accordance with Section 12(b). Notwithstanding the foregoing, in the event that any Statement of Work remains in effect following such termination or expiration, these Terms of Service shall govern and continue in effect with regard to such Statement of Work until the termination of such Statement of Work.

(b) Termination for Cause. Either Party may terminate these Terms of Service and/or Statement of Work for cause upon sixty (60) days' written notice of a material breach by the other Party of its obligations under these Terms of Service or the or Statement of Work, if such breach remains uncured at the expiration of such period.

(c) Effects of Termination. Upon termination of these Terms of Service or expiration of its Term: (i) the Parties shall work together in good faith to address any and all post-termination issues concerning these Terms of Service, including but not limited to the retrieval or destruction of Customer Data and each Party's Confidential Information, and (ii) all licenses granted to Customer hereunder with respect to the Services and Software shall automatically terminate and Customer shall immediately discontinue its use thereof. If Customer makes no written request regarding treatment of its Customer Data after termination or expiration of these Terms of Service within thirty (30) days prior to the date of termination, SolCyber shall have no obligation to maintain the Customer Data and will have no liability to Customer in respect of the same. If the Customer does make a written request for its Customer Data within such thirty (30) day period, SolCyber shall provide the Customer a written quote regarding the retrieval fee for such Customer Data ("Retrieval Fee") and will provide such Customer Data promptly, subject to the provision following regarding payment of outstanding fees and expenses. In the event Customer incurs any Retrieval Fees, any and all Retrieval Fees, and any and all unpaid fees and expenses incurred by the Customer in connection with the Services are due and payable to SolCyber immediately upon the date of termination and must be received by SolCyber prior to SolCyber providing such Customer Data to the Customer. In the event no request for Customer Data occurs within the thirty (30) day period and no Retrieval Fees are incurred, any and all unpaid fees and expenses incurred by the Customer in connection with the Services are due and payable immediately upon the date of termination. All subscription fees paid are non-refundable. Sections 1, 5-7, 8(b), 9, 12, and 14 shall survive any termination or expiration of these Terms of Service.

13 Equitable Relief.

The Parties agree that in the event of any breach or threatened breach of these Terms of Service; the non-breaching party may suffer an irreparable injury, such that no remedy at law will afford that party adequate protection against or appropriate compensation for such injury. Accordingly, in addition to remedies available at law, the Parties hereby agrees that the non-breaching party shall be entitled to seek specific performance as well as such injunctive relief as may be granted by a court of competent jurisdiction.

14 Miscellaneous

(a) Assignment. Neither Party may assign or transfer any of its rights or delegate any of its obligations hereunder, in each case whether voluntarily, involuntarily, by operation of law, or otherwise, without the prior written consent of the other Party, which consent shall not be unreasonably withheld, conditioned, or delayed; provided, however, that SolCyber may assign its rights or delegate its obligations, in whole or in part, without such consent to (i) one or more of its affiliates, or (ii) an entity that acquires all or substantially all of the business or assets of such Party to which these Terms of Service pertains, whether by merger, reorganization, acquisition, sale, or otherwise. Any purported assignment, transfer, or delegation in violation of this Section 14(a) will be null and void. No assignment, transfer, or delegation will relieve the assigning or dele- gating Party of any of its obligations hereunder. These Terms of Service are binding upon and inure to the benefit of the Parties hereto and their respective permitted successors and assigns.

(b) Amendment and Modification; Waiver. These Terms of Service may not be amended or modified except in a writing executed by duly authorized representatives of each Party. No waiver by any Party of any of the provisions hereof will be effective unless explicitly set forth in writing and signed by the Party so waiving. Except as otherwise set forth in these Terms of Service, (i) no failure to exercise, or delay in exercising, any rights, remedy, power, or privilege arising from these Terms of Service will operate or be construed as a waiver thereof and (ii) no single or partial exercise of any right, remedy, power, or privilege hereunder will preclude any other or further exercise thereof or the exercise of any other right, remedy, power, or privilege.

(c) Entire Terms of Service. These Terms of Service, together with any other documents incorporated herein by reference and all related Exhibits, constitutes the sole and entire agreement of the Parties with respect to the subject matter of these Terms of Service and supersedes all prior and contemporaneous understandings, agreements, and representations and warranties, both written and oral, with respect to such subject matter. In the event of any inconsistency between the statements made in the body of these Terms of Service, the related Exhibits, and any other documents incorporated herein by reference, such inconsistencies will be resolved as follows: the terms of the Order Form (described in the applicable Statement of Work) control as to all other documents, the terms of the Statement of Work control as to all other documents after the Order Form, and these Terms of Service controls as to all other documents after the Order Form and any Statement of Work.

(d) Force Majeure. In no event shall either Party be liable to the other Party, or be deemed to have breached these Terms of Service, for any failure or delay in performing its obligations under these Terms of Service, if and to the extent such failure or delay is caused by any circumstances beyond the other Party's reasonable control, including but not limited to acts of God, flood, fire, earthquake, explosion, pandemic, war, terrorism, invasion, riot or other civil unrest, strikes, labor stoppages or slowdowns or other industrial disturbances, or passage of law or any action taken by a govern- mental or public authority, including imposing an embargo.

(e) Governing Law. These Terms of Service are governed by and construed in accordance with the internal laws of the State of Texas without giving effect to any choice or conflict of law provision or rule that would require or permit the application of the laws of any jurisdiction other than those of the State of Texas. Any legal suit, action, or proceeding arising out of or related to these Terms of Service or the licenses granted hereunder will be instituted exclusively in the federal courts of the United States or the courts of the State of Texas, in each case located in the city of Dallas, and each Party irrevocably submits to the exclusive jurisdiction of such courts in any such suit, action, or proceeding. The Parties exclude in its entirety the application to these Terms of Service of the United Nations Convention on Contracts for the International Sale of Goods.

(f) Notices. All notices, requests, consents, claims, demands, waivers, and other communications hereunder (each, a "Notice") must be in writing. All Notices to SolCyber must be delivered by nationally recognized overnight courier (with all fees pre-paid) or certified or registered mail (in each case, return receipt requested, postage pre-paid) to the address set forth in the applicable order form, or by email to legal@solcyber.com (with confirmation of transmission). Except as otherwise provided in these Terms of Service, a Notice is effective only: (i) upon receipt by the receiving Party, and (ii) if the Party giving the Notice has complied with the requirements of this Section 14(f).

(g) Relationship of the Parties. The Parties to these Terms of Service are independent contractors and nothing in these Terms of Service will be deemed or construed as creating a joint venture, partnership, agency relationship, franchise, or business opportunity between SolCyber and Customer. Neither Party, by virtue of these Terms of Service, will have any right, power, or authority to act or create an obligation, express or implied, on behalf of the other Party.

(h) Severability. If any provision of these Terms of Service are invalid, illegal, or unenforceable in any jurisdiction, such invalidity, illegality, or unenforceability will not affect any other term or provision of these Terms of Service or invalidate or render unenforceable such term or provision in any other jurisdiction. These Terms of Service supersede any prior contemporaneous agreements or understandings between the parties hereto.

Exhibit A, Statement of Work, SolCyber Foundational Service

This Statement of Work ("**Foundational Services SOW**") is made by and between SolCyber Managed Security Services, Inc., a Delaware corporation, with offices at 1920 McKInney Ave., Suite 700, Dallas, TX 75201 ("**SolCyber**"), and the Customer executing an order form with SolCyber as of the date of such order form (the "**Effective Date**"). This Foundational Services SOW is entered into in connection with the Terms of Service accepted by Customer pursuant to an applicable order form (the "**Terms of Service**"). This Foundational Services SOW forms a part of and incorporates by reference all terms of the Terms of Service and all amendments thereto. Capitalized terms used but not defined in this Foundational Services SOW have the same meanings as provided in the Terms of Service. In addition, "you" and "your" as used in this document refer to Customer, and "we," "us," and "our" refer to SolCyber. SolCyber and Customer agree as follows:

I. Scope and Description of Services

1. Scope of Services

The SolCyber Foundational Security Services ("**Foundational Service**") provides a set of security services to the Customer to protect from modern cyber threats via SolCyber's Security Operations Center ("**SOC**"). SolCyber and Customer shall work together during a discovery phase to develop a mutually agreeable written program plan and schedule to address implementation of the Foundational Services (the "**Program Plan**"). The Program Plan shall address, among other things:

- Project kick-off and preparation for Foundational Service;
- SolCyber review of Customer's environment and inventory;
- Changes in systems and process to collect telemetry from the Customer's environment;
- Schedule for delivery, implementation, or transition (as may be applicable) of each Foundational Service offering; and
- Customer responsibilities under the Program.

Foundational Service includes the following services:

24/7 Monitoring Service

The SolCyber 24/7 Monitoring Service ("**Monitoring Service**") provides SOC capabilities including cyber security monitoring, advanced threat detection, human-led threat hunting, incident investigation, and response ("**SOC Services**"). The SOC Services are facilitated by a cloud-native, data science driven, co-managed technology platform ("**SolCyber SOC**"). The

SOC Services are delivered by SolCyber with either remote staff or those physically located together, or a combination thereof.

Coverage: Monitoring Service covers all technologies provided by Foundational Services, Extended Services and Device Monitoring Service purchased by the Customer that are on the supported product list.

1. *Log Collection* – Logs are collected by the SolCyber SOC and are made available for 365 days before they are deleted from the system. SolCyber reserves the right to adjust fees if such logs collected are more than the logs considered normal for infrastructure of average verbosity.
2. *Alert Analysis and Triage* – SolCyber will analyze logs on a 24x7x365 basis for signs of malicious activity. Suspicious alerts will be triaged by SolCyber and escalated as an incident if confirmed.
3. *Incident Alerting* – Upon confirmation of an incident, SolCyber will create an incident in the SolCyber SOC and notify the Customer within the provided SLA.
4. *Portal Access* – Incidents will be made available via an online portal or other means at the discretion of SolCyber.

Log Collection Device – Customers can purchase one or more Log Collection Devices as needed and at their option. However, this device may be required for certain technologies on the supported product list. Ownership of the Log Collection Device will be transferred to the Customer upon shipment. Alternatively, the Customer can purchase their own supported hardware or virtual infrastructure.

Advanced Email Protection Service

The SolCyber™ Advanced Email Protection (“AEP Service”) provides protection against modern email threats including phishing attacks, business email compromise and email fraud. The AEP Service includes a cloud native, multi-vector detection enabled email solution which is also managed by the SolCyber SOC.

Coverage: The AEP Service supports the included email technology or others approved and supported by SolCyber.

AEP License: The AEP Service includes licenses for an email solution. The Customer can deploy the email solution for up to the number of User licenses purchased for the Foundational Service.

1. *Remote Implementation* – SolCyber will work with the Customer to remotely implement the included email technology. Customer is expected to support the activities outlined in the AEP on-boarding guide.

2. *Policy Configuration and Management* – SolCyber will update the email solution's configurations based off best practices and input from the Customer including black and whitelisting.
3. *Quarantine Management* – SolCyber will respond to requests to release emails from quarantine within the provided SLA.
4. *System Availability* – SolCyber will undertake reasonable measures to ensure that the AEP Service availability meets or exceeds the provided SLA.
5. *Performance and Availability Monitoring* – The email solution will be monitored 24x7x365 for anomalies in performance or availability. Upon confirmation of a fault, SolCyber will create an incident in the SolCyber SOC and notify the Customer within SLA.

Endpoint Protection and Response Service

The SolCyber™ Endpoint Protection and Response ("**Endpoint Service**") provides protection against endpoint threats including threat detection, remote response and remediation assistance. The Endpoint Service is powered by a bundled endpoint solution.

Coverage: The Endpoint Service supports the included bundled or other endpoint protection and endpoint detection and response ("**EDR**") technologies approved and supported by SolCyber.

Endpoint Licenses: The Endpoint Service includes licenses for bundled endpoint solution. The Customer can deploy EDR on any Endpoint up to 1.25 times the User licenses purchased for Foundational Service. An Endpoint is defined to include any host machine running supported versions of Linux, Windows, or MacOS operating systems to include servers, virtual servers, user workstations, and laptops. The Customer will be invoiced for additional license capacity as needed based on Section II below.

1. *Remote Implementation* – SolCyber will work with the Customer to remotely implement the included bundled technology. Customer is expected to support the activities outlined in the Endpoint Service on-boarding guide.
2. *Policy Configuration and Management* – SolCyber will update EDR's configurations based off best practices and input from the Customer including device blocking.
3. *Response* – SolCyber will connect to confirmed incidents by remotely connecting to endpoints with EDR to perform additional triage, containment and response work when possible.
4. *EDR Troubleshooting* – SolCyber will respond to requests to troubleshoot issues related to EDR within the provided SLA.
5. *System Availability* – SolCyber will undertake reasonable measures to ensure that the EDR availability meets or exceeds the provided SLA.

6. *Performance and Availability Monitoring* – The EDR will be monitored 24x7x365 for anomalies in performance or availability. Upon confirmation of a fault, SolCyber will create an incident in the SolCyber SOC and notify the Customer within 4 hours.

DNS Protection Service

The SolCyber™ DNS Protection Service ("DNS Service") protects endpoints from web-based threats. The DNS Service is powered by a bundled endpoint solution.

Coverage: The DNS Service supports the included bundled or other cloud-based DNS technologies approved and supported by SolCyber.

Endpoint Licenses: The DNS Service includes licenses for bundled endpoint solution. The Customer can deploy DNS agent on any Endpoint up to 1.25 times the User licenses purchased for Foundational Service. An Endpoint is defined to include any host machine running supported versions of Linux, Windows, or MacOS operating systems to include servers, virtual servers, user workstations, and laptops. The Customer will be invoiced for additional license capacity as needed based on Section II below.

1. Remote Implementation – SolCyber will work with the Customer to remotely implement the included bundled technology. Customer is expected to support the activities outlined in the DNS Service on-boarding guide.
2. Policy Configuration and Management – SolCyber will update DNS configurations based off best practices and input from the Customer to block access to malicious websites. Content filtering is available to the Customer for an additional $0.50/user.
3. Content Filtering – Customers can leverage the platform to restrict user access to specific types of content including pornography. This is a self-serve service and available as an option at $0.50/user.
4. DNS Troubleshooting – SolCyber will respond to requests to troubleshoot issues related to EDR within the provided SLA.
5. System Availability – SolCyber will undertake reasonable measures to ensure that the DNS availability meets or exceeds the provided SLA.
6. Performance and Availability Monitoring – The DNS will be monitored 24x7x365 for anomalies in performance or availability. Upon confirmation of a fault, SolCyber will create an incident in the SolCyber SOC and notify the Customer within 4 hours.

Practical Vulnerability Management Service

The SolCyber™ Practical Vulnerability Management Service ("VM Service") provides the customer with a prioritize list of vulnerabilities to assist with patch management.

Coverage: The VM Service only supports the bundled vulnerability management technology.

Endpoint Licenses: The VM Service includes licenses for bundled vulnerability management solution. The Customer can deploy the VM Service agent on any Endpoint up to 1.25 times the Standard User licenses purchased for Foundational Service. An Endpoint is defined to include any host machine running supported versions of Linux, Windows, or MacOS operating systems to include servers, virtual servers, user workstations, and laptops. The Customer will be invoiced for additional license capacity as needed based on Section II below. Non-endpoint Users are excluded.

1. Remote Implementation – SolCyber will work with the Customer to remotely implement the included bundled technology. Customer is expected to support the activities outlined in the Endpoint Service on-boarding guide.
2. Monthly Reporting – SolCyber will provide a monthly report of critical patches to apply including status of patches from the previous month. Patches not applied within 30 days will be highlighted. Customer can opt-in for a monthly report of all vulnerabilities for compliance, but these will not be tracked.
3. Emergency Patch Alerting – SolCyber will alert the customer of new critical and exploitable vulnerabilities that require out-of-band patching.
4. VM Troubleshooting – SolCyber will respond to requests to troubleshoot issues related to VM within the provided SLA.
5. System Availability – SolCyber will undertake reasonable measures to ensure that the VM availability meets or exceeds the provided SLA.
6. Performance and Availability Monitoring – The VM Service will be monitored 24x7x365 for anomalies in performance or availability. Upon confirmation of a fault, SolCyber will create an incident in the SolCyber SOC and notify the Customer within 4 hours.

Phishing Simulation and Training Service

The SolCyber™ Phishing Simulation and Training ("Phishing Service") increases the security awareness of your employees through a combination of phishing email simulations and security awareness training. The Phishing Service is powered by a phishing and training solution.

Coverage: The Phishing Service supports the included phishing training solution or other technologies approved and supported by SolCyber.

Endpoint Licenses: The Phishing Service includes licenses for the phishing training solution. The Customer can deploy up to the number of User licenses purchased for the Foundational Service.

1. *Remote Implementation* – SolCyber will work with the Customer to remotely implement the included bundled technology. Customer is expected to support the activities outlined in the Phishing Service on-boarding guide.
2. *Phishing Simulation* – SolCyber will perform one phishing simulation exercise for the Customer every quarter via email.
3. *Phishing Training* – SolCyber will send associated phishing training to every user who fails the phishing simulation.
4. *Portal Access* – Training will be made available via an online portal

Ransomware Readiness Assessment Service

The SolCyber™ Ransomware Readiness Assessment Service ("Readiness Service") assessing the Customer's environment to determine the likelihood of a successful ransomware attack.

1. *Assessment* – SolCyber will work with the Customer to assess various security controls within the environment. Customer is expected to support the activities outlined in the Readiness Service on-boarding guide. The assessment will be performed once a year.
2. *Report* – SolCyber will deliver a report including recommendations on changes to improve the Customer's security posture.

Active Directory Assessment Service

The SolCyber™ Active Directory Assessment Service ("ADS Service") assesses the Customer's Active Directory environment for misconfigurations and vulnerabilities. The AD Service is powered by bundled Active Directory assessment tool.

Coverage: The ADP Service supports the included solution or others as approved and supported by SolCyber. The service is only available for Customers with Active Directory or Azure AD.

1. *Assessment* – SolCyber will work with the Customer to assess various security controls within Active Directory. Customer is expected to support the activities outlined in the ADS Service on-boarding guide. The assessment will be performed up to twice a year.
2. *Report* – SolCyber will deliver a report including recommendations on changes to improve the Customer's security posture.

Other Security Logs Service

The SolCyber™ Other Security Logs Service ("Other Logs Service") provides support for monitoring of additional log sources.

Coverage: Monitoring of logs from technologies in the SolCyber Supported Products List ("SPL") for Other Logs Service are included in the coverage for SolCyber's 24/7 Monitoring

Service (“Monitoring Service”). This is limited to a total of one (1) Gigabyte per day ("GB/Day"), as measured on an average basis each calendar month. If actual usage exceeds one (1) GB/Day for a given month, then SolCyber reserves the right to request that the Customer purchase Security Logs Add-on Service within thirty (30) days of providing notification and a quote to provide such additional extended service.

For all services that are included in Foundational Service, SolCyber reserves the right to substitute a SolCyber approved and supported product and solution, with a minimum of 30 days’ notice of a plan to effect such change in its operations and delivery of Foundational Service.

2. *Term.* This Foundational Services SOW shall commence on the Effective Date and continue for the term set forth in the applicable order form unless and until either Party gives notice of termination, as provided for in the Terms of Service.

3. *Assumptions.* Our pricing assumes that the Customer does not require protection for excessive non-user email addresses, or excessive domains. If there are requirements above a “normal” level of protection, then SolCyber reserves the right to adjust its price, or not cover such addresses or domains. Further, Customer agrees that it is responsible for providing all reasonable cooperation and assistance, including timely performance of required tasks identified in the Program Plan. SolCyber will work with Customer to monitor delays in the Program Plan and work together to mitigate risks. In no event shall SolCyber be responsible or liable for any delay or failure of performance caused in whole or in part by Customer’s delay in performing, or failure to perform, any of its obligations under the Terms of Service (including in any Program Plan).

4. *Service Levels Agreement.* The purpose of this section is to describe the relevant actions, expectations, remedies, and exclusions related to the performance of Foundational Service. The Service Level Agreement (“SLA”) is as follows:

SolCyber SOC SLAs:

SLA	Item	What It Is	Target Uptime
1	SOC Availability	Percent of minutes in a 1-month period	>=99.5%

The following definitions apply to this SLA:

- *“Downtime”* means Customer is not able to log in to SolCyber SOC and view a incident.

- *"Monthly Uptime Percentage"* means total number of minutes in a month (calculated as number of days in the applicable month x 24 hours x 60 minutes), minus the number of minutes suffered from Downtime in a month, divided by the total number of minutes in the month excluding periods of Planned Maintenance (Excused Downtime).
- *"Planned Maintenance"* will not count against Uptime and means any unavailability, suspension or termination to the extent caused by: (i) factors outside of SolCyber's reasonable control, including any force majeure event or Internet access or related problems beyond the demarcation point of SolCyber; (ii) any actions or inactions of Customer or any third party; (iii) SolCyber's suspension and/or termination of Customer's right to use the Service; (iv) any planned downtime or maintenance that SolCyber or its authorized service providers performs on the Service, provided that (a) Customer is notified at least seven days in advance or (b) Customer has agreed to the date and time of such non-emergency maintenance; or (v) any periods of shutdown necessitated by emergency maintenance.
- SolCyber reserves the right to disable any Customer's rules and/or require them to be tuned to maintain this SLA.

Customer will be eligible to receive the financial credits described below if SolCyber SOC falls below a Monthly Uptime Percentage of 99.5%. Credits will be calculated once at the end of each month.

Monthly Uptime Percentage	Monthly Uptime SLA Credit
>= 99.5%	No Credit
99.1% - < 99.5%	$0.40/user
< 99.1%	$1.20/user

Credits are calculated based off the number of subscribed Users to the Foundational Service.

SLA	Item	What It Is	Response Time Target
2	Mean Time to Triage - Suspicious Entity SLA	SolCyber will create Security Incident Case in SolCyber SOC	within 3 hours during the business day (defined as 9am to 5pm Eastern Time) of when a Critical/High Severity Suspicious Entity is created/triggered.

3	Mean Time to Escalate - Security Incident SLA	SolCyber will escalate Security Incident Cases to Customer	Within 1 hour during the business day (defined as 9am to 5pm Eastern Time) after it is assigned an Impact level of Sev-1, and within 3 hours after it is assigned an Impact level of Sev-2 in SolCyber SOC.
4	Mean Time to Troubleshoot – Technical Support SLA	SolCyber will begin troubleshooting "Technical Support Cases"	Within 3 business hours (defined as 9am to 5pm Eastern Time). For issues reported after the business day, troubleshooting will begin the next business day.

Security Incident Cases are considered escalated when either SolCyber changes the status to "Escalated to Customer" in SolCyber SOC or when an equivalent case/incident/ticket is created and linked in Customer's 3rd party case management system that is integrated with SolCyber SOC.

Exclusions from coverage under this SLA:

- Suspicious Entities generated by one or more newly published Detection rules are excluded from this SLA until 7 days after the rule is published in SolCyber SOC ("Rule Probationary Period"). During the Rule Probationary Period, Suspicious Entities generated by newly published rules will still be monitored, triaged and investigated.
- Suspicious Entities generated by any Customer rules created by Customer in SolCyber SOC
- Suspicious Entities discovered during any Rule Probationary Period by newly developed rules and analytical models that are triggered by retroactive scans of existing logs as far back as 31 days.
- During the onboarding period following Service Activation (the "Service Adjustment Period"), SLAs will not apply. The Customer will receive a notification regarding the transition to maintenance upon the completion of the onboarding period, at which point SLAs will apply.
- Should a log collector fail, SLAs will not apply during the period when the collector is unavailable.

- SLAs do not apply during maintenance windows or in the event of any Customer-caused service outage that prohibits or otherwise limits SolCyber from providing the Service, including, but not limited to, Customer misconduct, Custom rule execution that results in Downtime for SolCyber SOC, negligence, inaccurate or incomplete information, and modifications made to the Service, hardware, or software by Customers, their employees or third parties acting on behalf of Customer. Maintenance windows ("Planned Maintenance Windows") for SolCyber SOC will be limited to a maximum of four hours per week (7-day period) unless communicated in writing by SolCyber.
- SLAs do not apply in the event Customer does not fulfil and comply with responsibilities and conditions set forth in this Foundational Services SOW.

The Customer will be eligible for $0.40 per User of Foundational Service for each violation of SLA 2, 3 or 4.

Customer will be eligible to receive the financial credits described below if SolCyber AEP SLA's fall below the Target Uptimes specified:

SLA	Item	What It Is	Target Uptime
5	Security Portal & API Availability	Percent of hours in a rolling 12-month period	99.95%
6	Security Service Availability	Percent of hours in a rolling 12-month period that the security service is operational	99.95%

The following definitions apply to this SLA:

- Measurement of the above SLAs will occur on a rolling 12-month basis, at the end of each calendar month.
- "Uptime" availability will be measured as the aggregate number of minutes during a year in which the AEP Service was available divided by the total number of minutes in the year (calculated as 365 days x 24 hours x 60 minutes) excluding periods of Planned Maintenance (Excused Downtime).
- "Planned Maintenance" will not count against Uptime and means any unavailability, suspension or termination to the extent caused by: (i) factors outside of SolCyber's reasonable control, including any force majeure event or Internet access or related problems beyond the demarcation point of SolCyber; (ii) any actions or inactions of Customer or any third party; (iii) SolCyber's suspension and/or termination of Customer's right to use the AEP Service; (iv) any planned downtime or maintenance that SolCyber or its authorized service providers performs on the AEP Service,

provided that (a) Customer is notified at least seven days in advance or (b) Customer has agreed to the date and time of such non-emergency maintenance; or (v) any periods of shutdown necessitated by emergency maintenance.

The Customer will be eligible for $0.40 per User of Foundational Service for each 24-hour period the service is unavailable.

SLA	Item	What It Is	Response Time Target
7	Mean Time to Respond – Quarantine Email SLA	SolCyber will respond to quarantined email release request from the Customer	Within 4 business hours from receiving an approved request (soc@solcyber.com or a ticket request) submitted to the SOC. If the request is received within 4 business hours of a 5pm Eastern Time SOC operations cut-off, then the response shall be considered timely if completed within the next business day
8	"Mean Time to Respond – EDR Troubleshooting"	SolCyber will respond to troubleshoot request from the Customer for the endpoint protection and endpoint detection and response technology	Within 4 business hours from receiving an approved request (soc@solcyber.com or a ticket request) submitted to the SOC. If the request is received within 4 business hours of a 5pm Eastern Time SOC operations cut-off, then the response shall be considered timely if completed within the next business day
9	"Mean Time to Respond – Attivo Troubleshooting"	SolCyber will respond to troubleshoot request from the Customer for the Attivo agent.	Within 4 business hours from receiving an approved request (soc@solcyber.com or a ticket request) submitted

			to the SOC. If the request is received within 4 business hours of a 5pm SOC operations cut-off, then the response shall be considered timely if completed within the next business day
10	"Mean Time to Respond – VM Troubleshooting"	SolCyber will respond to troubleshoot request from the Customer for the VM agent.	Within 4 business hours from receiving an approved request (soc@solcyber.com or a ticket request) submitted to the SOC. If the request is received within 4 business hours of a 5pm Eastern Time SOC operations cut-off, then the response shall be considered timely if completed within the next business day

The Customer will be eligible for $0.40 per User of Foundational Service for each violation of SLA 7 or 8.

Claim For Credit:

- Customer must submit a Credit request to SolCyber within 30 days of the end of the calendar month in which SolCyber fails to meet the standards provided in this Section.
- Said Credit request needs to include details and dates of the relevant anomalies and Customer must cooperate with SolCyber's investigation of the Credit request as may be necessary and reasonably requested by SolCyber.
- Customer must accrue a minimum amount of $100 in Credit before SolCyber will credit back any amounts, and Credits may not be used to set off any outstanding invoices or payments due at the time of request.

The parties agree that the above Credits constitute compensation to Customer in the form of a credit to the Customer's next invoice or a future invoice, and not a penalty. The parties acknowledge and agree that i) Customer's harm caused by SolCyber delayed delivery of the Services would be impossible or very difficult to accurately estimate as of the Effective Date, ii) the Financial Credit amounts set forth above are a reasonable estimate of the anticipated or actual harm that might arise from SolCyber's breach of its Service availability obligations; and iii) SolCyber's payment or credit of these amounts constitute SolCyber's sole liability and entire obligation and Customer's exclusive remedy for SolCyber's breach of its Service availability obligations.

II. PRICING & PAYMENT TERMS

1. Fees:

SolCyber will invoice Customer in US Dollars based on a fixed fee for a stated and fixed level of consumption according to the applicable order form. While the Customer's actual consumption may be measured to be less than what is invoiced for any month, and SolCyber shall measure such consumption periodically over the term of the Foundational Services SOW, the Customer acknowledges and agrees that it is paying for a fixed consumption of resources provided by SolCyber, and there will not be any credit provided for such difference. However, should the Customer's actual consumption exceed the fixed consumption being invoiced, then SolCyber shall have the contractual right to propose an adjustment to the fixed fee amounts to consider a higher level of consumption, and further shall provide the Customer an opportunity to reduce the resources consumed to bring such amounts within the then current fixed levels within a 30-day period. SolCyber shall propose this new amount to the Customer for agreement, and it shall be documented in the form of an amendment or change order to the applicable order form.

A "**User**" is defined as a person in your organization with an individually assigned email address. SolCyber will validate this user count periodically by the total number of Customer email addresses included in Office365 or G Suite / Google Workspace / or equivalent. The User count will only include those Users active within the last thirty monitored days, as of the date measured, and will include service accounts and shared mailboxes, but not distribution lists.

The Monthly Fixed Fee for Foundational Service allows for the Customer to use up to an additional 25% more Endpoints if users have more than one device. This applies to both Endpoint, VM Service and DNS Services. "Endpoint" is defined to include any host machine running a support version of Linux, Windows, or MacOS operating systems to include servers, virtual servers, user workstations, and laptops. If Customer exceeds said licenses, the Customer will be invoiced for the difference in Endpoint licenses the following month for $15 per Endpoint or as otherwise stated in the applicable order form.

In the event In any calendar month that the Customer's actual data usage under Monitoring Service exceeds 1 Gigabyte per day for that month, and the Customer has not then agreed to add the Security Logs Service within the required thirty (30) day notice period, then SolCyber shall be entitled to include in its next monthly Invoice an amount representing the additional monthly fee equal to result of the quantity of Gigabytes per day consumed In the month that exceeds the 1 Gigabyte per day limit multiplied times $200. The actual usage shall first be rounded down to the nearest whole number. The actual measurement of GB/Day shall be based on the monthly average. SolCyber shall continue to invoice monthly for excess usage above 1 Gigabyte per day so long as such excess usage exists in any calendar month.

Customers can purchase Log Collection Devices as needed to support log collection. The first Log Collection Device is included at no charge. Additional Log Collection Devices will be charged at $1,000 per unit, not including applicable taxes. Customer shall be responsible for shipping and insurance fees to their physical location. Billing will occur upon shipment, and payment will be due immediately.

Customer can request a copy of all Customer Data held by SolCyber at the termination of its contract at an additional fee. The Retrieval Fee will the total amount of Data retained by SolCyber in Gigabytes (GB) computed at $1.00/GB, plus a flat $1,500 processing fee. The request for Data must be submitted no less than thirty (30) days before the end of service date. If the Customer agrees with the Retrieval Fee, then SolCyber shall Immediately invoice for such amount, and payment must be made to SolCyber, along with payment of any other outstanding fees and expenses, prior to any Customer Data being released to the Customer.

The commencement dates for each of the Foundational Services may differ from one another and from the Effective Date of the Foundational Services SOW. Notwithstanding these differences in commencement dates, there shall be no credit or refund provided for any month with one or more elements of services not yet transitioned.

2. Expenses:

The fees and rates noted in Section II, Item 1 do not include any travel or other costs directly authorized by the Customer in advance in connection with the provision of services under this Foundational Services SOW. Should the Customer authorize SolCyber in writing to incur such additional travel or other costs, then SolCyber shall include in the next monthly invoice such costs following their incurrence.

3. Invoicing and Payment Terms:

Unless otherwise provided in the applicable order form, invoicing shall occur on the last day of each calendar month during the Foundational Services SOW term reflecting services incurred for that calendar month provided, however, that the initial invoice shall be prorated for the period between the Effective Date and the last day of the first calendar month of the Foundational Services SOW term, and any final invoice shall be prorated for the number of calendar days in which services were provided in the final month of the Foundational Services SOW. Unless otherwise provided In the applicable order form, all invoices are due within thirty (30) days of the invoice date.

Exhibit D, Statement of Work, SolCyber Cloud Protection Service

This Statement of Work ("**Cloud Protection Service SOW**") is made by and between SolCyber Managed Security Services, Inc., a Delaware corporation, with offices at 1920 McKInney Ave., Suite 700, Dallas, TX 75201 ("**SolCyber**"), and the Customer executing an order form with SolCyber as of the date of such order form (the "**Effective Date**"). This Cloud Protection Services SOW is entered into in connection with the Terms of Service accepted by Customer pursuant to an applicable order form (the "**Terms of Service**"). This Cloud Protection Services SOW forms a part of and incorporates by reference all terms of the Terms of Service and all amendments thereto. Capitalized terms used but not defined in this Cloud Protection Services SOW have the same meanings as provided in the Terms of Service. In addition, "you" and "your" as used in this document refer to Customer, and "we," "us," and "our" refer to SolCyber. SolCyber and Customer agree as follows:

I. Scope and Description of Services

1. Scope of Services

The SolCyber Cloud Protection and Visibility Service ("Cloud Protection Service") detects threats in the Customer's cloud environment and provides on-going advice to strengthen its security. The Cloud Service is powered by a bundled cloud security solution. Cloud Protection Service is an Extended Service and can only be utilized if the Customer is using Foundational Service.

Coverage: The Cloud Service supports the included software solution or others as approved and supported by SolCyber. Cloud support available for AWS, Azure and Google Cloud Platform.

Cloud Licenses: The Cloud Service includes licenses for scanning of cloud infrastructure. The service is used to secure 'Resources'. A Resource in defined as any of the resources listed in the table below:

Compute Resources
EC2 instances
Lambda function configurations*
EKS clusters
ECS services
Data Resources
S3 buckets

RDS instances
DynamoDB tables

*Note: Every 10 Lambda function configuration Resource shall count as 1 Resource for invoicing purposes.

A. *Security Monitoring* – Resourced licensed for Cloud Protection Service are included in the coverage for SolCyber's 24/7 Monitoring Service ("Monitoring Service").

B. *Remote Implementation* – SolCyber will work with the Customer to remotely implement the included bundled technology. Customer is expected to support the activities outlined in the Cloud Service on-boarding guide.

C. *Policy Configuration and Management* – SolCyber will update the solution's configurations based off best practices and input from the Customer including policy tuning.

D. *Best Practice Recommendations* – SolCyber will perform an assessment of the cloud infrastructure on a periodic basis against but not limited to CIS, PCI and SOC2 benchmarks. Findings will be presented to the Customer in the form of a report.

E. *Troubleshooting* – SolCyber will respond to requests to troubleshoot issues related to the solution's agent within the provided SLA.

F. *System Availability* – SolCyber will undertake reasonable measures to ensure that the solution's availability meets or exceeds the provided SLA.

G. *Performance and Availability Monitoring* – The solution will be monitored 24x7x365 for anomalies in performance or availability. Upon confirmation of a fault, SolCyber will create an incident in the SolCyber SOC and notify the Customer within 4 hours.

2. **Term**

This Cloud Protection Services SOW shall commence on the Effective Date and continue for the term set forth in the applicable order form unless and until either Party gives notice of termination, as provided for in the Terms of Service.

3. **Assumptions**

Customer agrees that it is responsible for providing all reasonable cooperation and assistance, including timely performance of required tasks identified in the Program Plan. SolCyber will work with Customer to monitor delays in the Program Plan and work together to mitigate risks. In no event shall SolCyber be responsible or liable for any delay or failure of performance caused in whole or in part by Customer's delay in performing, or failure to perform, any of its obligations under the Terms of Service (including in any Program Plan).

II. PRICING & PAYMENT TERMS

1. Fees:

SolCyber will invoice Customer in US Dollars based on a fixed fee for a stated and fixed level of consumption according to the applicable order form. While the Customer's actual consumption may be measured to be less than what is invoiced for any month, and SolCyber shall measure such consumption periodically over the term of the Cloud Protection Service SOW, the Customer acknowledges and agrees that it is paying for a fixed consumption of resources provided by SolCyber, and there will not be any credit provided for such difference.

The Cloud Protection Service provides that the customer can utilize 50 Resources for every Resource Bucket of Cloud Protection Service purchased. If the Customer's actual number of Resources measured at the end of month exceeds the total included number of Resources (Number of Resource Buckets x 50), then the Customer will be invoiced for the additional Resource Buckets consumed, which is determined by taking the exceeded quantity of Resources, dividing by 50 and rounding up to the nearest whole number. The invoice will be charged at the Resource Bucket rate listed in the latest Order Form.

The commencement dates for each of the Cloud Protection Service may differ from one another and from the Effective Date of the Cloud Protection Service SOW. Notwithstanding these differences in commencement dates, there shall be no credit or refund provided for any month with one or more elements of services not yet transitioned.

2. Expenses:

The fees and rates noted in Section II, Item 1 do not include any travel or other costs directly authorized by the Customer in advance in connection with the provision of services under this Cloud Protection Service SOW. Should the Customer authorize SolCyber in writing to incur such additional travel or other costs, then SolCyber shall include in the next monthly invoice such costs following their incurrence.

3. Invoicing and Payment Terms:

Unless otherwise provided in the applicable order form, invoicing shall occur on the last day of each calendar month during the Cloud Protection Services SOW term reflecting services incurred for that calendar month provided, however, that the initial invoice shall be prorated for the period between the Effective Date and the last day of the first calendar month of the Cloud Protection Services SOW term, and any final invoice shall be prorated for the number of calendar days in which services were provided in the final month of the Foundational Cloud Security Service SOW. Unless otherwise provided In the applicable order form, all invoices are due within thirty (30) days of the invoice date.

Exhibit E, Statement of Work, SolCyber Security Logs Add-on Service

This Statement of Work (“**Security Logs Add-on Service SOW**”) is made by and between SolCyber Managed Security Services, Inc., a Delaware corporation, with offices at 1920 McKInney Ave., Suite 700, Dallas, TX 75201 ("**SolCyber**"), and the Customer executing an order form with SolCyber as of the date of such order form (the “**Effective Date**”). This Security Logs Add-on Service SOW is entered into in connection with the Terms of Service ed by Customer pursuant to an applicable order form (the “**Terms of Service**”). This Security Logs Add-on Service SOW forms a part of and incorporates by reference all terms of the Terms of Service and all amendments thereto. Capitalized terms used but not defined in this Security Logs Add-on Service SOW have the same meanings as provided in the Terms of Service. In addition, “you” and “your” as used in this document refer to Customer, and “we,” “us,” and “our” refer to SolCyber. SolCyber and Customer agree as follows:

I. Scope and Description of Services

1. Scope of Services

The SolCyber Security Logs Add-on Service (“Security Logs Service”) provides security monitoring for the supported logging technologies. Security Logs Service is an Extended Service and can only be purchased if the Customer is using Foundational Service, MDR+ Services or XDR++ Services.

Coverage: Monitoring of logs from technologies in the SolCyber Supported Products List (“SPL”) for Security Logs Service are included in the coverage for SolCyber’s 24/7 Monitoring Service (“Monitoring Service”).

2. Term.

This Security Logs Add-on Service SOW shall commence on the Effective Date and continue for the term set forth in the applicable order form unless and until either Party gives notice of termination, as provided for in the Terms of Service.

3. Assumptions

Our pricing assumes that the Customer does not require protection for excessive non-user email addresses, or excessive domains. If there are requirements above a “normal” level of protection, then SolCyber reserves the right to adjust its price, or not cover such addresses or domains. Further, Customer agrees that it is responsible for providing all reasonable cooperation and assistance, including timely performance of required tasks identified in the Program Plan. SolCyber will work with Customer to monitor delays in the Program Plan and work together to mitigate risks. In no event shall SolCyber be responsible or liable for any delay or failure of performance caused in whole or in part by Customer’s delay in performing, or failure to perform, any of its obligations under the Terms of Service (including in any Program Plan).

II. PRICING & PAYMENT TERMS

1. Fees:

SolCyber will invoice Customer in US Dollars based on a fixed fee for a stated and fixed level of consumption according to the applicable order form. While the Customer's actual consumption may be measured to be less than what is invoiced for any month, and SolCyber shall measure such consumption periodically over the term of the Security Logs Add-on Service, the Customer acknowledges and agrees that it is paying for a fixed consumption of resources provided by SolCyber, and there will not be any credit provided for such difference. However, should the Customer's actual consumption exceed the fixed consumption being invoiced, then SolCyber shall have the contractual right to propose an adjustment to the fixed fee amounts to consider a higher level of consumption, and further shall provide the Customer an opportunity to reduce the resources consumed to bring such amounts within the then current fixed levels within a 30-day period. SolCyber shall propose this new amount to the Customer for agreement, and it shall be documented in the form of an amendment or change order to the applicable order form.

The Security Logs Service provides the customer can utilize 50 Events Per Second ("EPS") for every bucket of Security Logs Service purchased, or "EPS Bucket". If the Customer's total EPS utilized at the end of each calendar month should exceed the total included number of EPS (number of buckets times 50), then SolCyber, in accordance with the preceding paragraph, may propose an adjustment to increase the EPS Bucket quantity to invoice for additional capacity.

Customers can purchase Log Collection Devices as needed to support log collection. The first Log Collection Device is included at no charge. Additional Log Collection Devices will be charged at $1,000 per unit, not including applicable taxes. Customer shall be responsible for shipping and insurance fees to their physical location. Billing will occur upon shipment, and payment will be due immediately.

The commencement dates for each of the Security Logs Service may differ from one another and from the Effective Date of the Security Logs Add-on Service SOW. Notwithstanding these differences in commencement dates, there shall be no credit or refund provided for any month with one or more elements of services not yet transitioned.

2. Expenses:

The fees and rates noted in Section II, Item 1 do not include any travel or other costs directly authorized by the Customer in advance in connection with the provision of services under this Security Logs Add-on Service SOW. Should the Customer authorize SolCyber in writing to incur such additional travel or other costs, then SolCyber shall include in the next monthly invoice such costs following their incurrence.

3. Invoicing and Payment Terms:

Unless otherwise provided in the applicable order form, invoicing shall occur on the last day of each calendar month during the Security Logs Add-on Service SOW term reflecting services incurred for that calendar month provided, however, that the initial invoice shall be prorated for the period between the Effective Date and the last day of the first calendar month of the Security Logs Add-on Service SOW term, and any final invoice shall be prorated for the number of calendar days in which services were provided in the final month of the Foundational Cloud Security Service SOW. Unless otherwise provided In the applicable order form, all invoices are due within thirty (30) days of the invoice date.

Exhibit G, Statement of Work, SolCyber Incidence Response Monitoring Services

This Statement of Work ("Incidence Response **Monitoring Services SOW**") is made by and between SolCyber Managed Security Services, Inc., a Delaware corporation, with offices at 1920 McKInney Ave., Suite 700, Dallas, TX 75201 ("**SolCyber**"), and the Customer executing an order form with SolCyber as of the date of such order form (the "**Effective Date**"). This IRM Services SOW is entered into in connection with the Terms of Service accepted by Customer pursuant to an applicable order form (the "**Terms of Service**"). This Monitoring Services SOW forms a part of and incorporates by reference all terms of the Terms of Service and all amendments thereto. Capitalized terms used but not defined in this Monitoring Services SOW have the same meanings as provided in the Terms of Service. In addition, "you" and "your" as used in this document refer to Customer, and "we," "us," and "our" refer to SolCyber. SolCyber and Customer agree as follows:

I. Scope and Description of Services

SolCyber

1. Scope of Services

The SolCyber Incident Response Monitoring Services (“**IRM Service**”) provides a set of security services to the Customer to protect their customer ("End Customer") from modern cyber threats via SolCyber’s Security Operations Center (“**SOC**”). SolCyber and Customer shall work together during a discovery phase to develop a mutually agreeable written program plan and schedule to address implementation of the IRM Services (the “**Program Plan**”). The Program Plan shall address, among other things:

- Project kick-off and preparation for IRM Service;
- Changes in systems and process to collect telemetry from the Customer’s environment;
- Overview of the state of the End Customer’s environment and incident response engagement to date;
- Schedule for delivery, implementation, or transition (as may be applicable) of each IRM Service offering; and
- Customer responsibilities under the Program.

IRM Service shall be limited to a time period of 45 days from hand-off of the EDR technology, and includes the following:

24/7 Monitoring Service

The SolCyber 24/7 Monitoring Service (“**Monitoring Service**”) provides SOC capabilities including cyber security monitoring, advanced threat detection, human-led threat hunting, incident investigation, and response (“**SOC Services**”). The SOC Services are facilitated by a cloud-native, data science driven, co-managed technology platform (“**SolCyber SOC**”). The SOC Services are delivered by SolCyber with either remote staff or those physically located together, or a combination thereof.

Coverage: Monitoring Service covers all technologies provided by IRM Services, Extended Services and Device Monitoring Service purchased by the Customer that are on the supported product list.

1. *Log Collection* – Logs are collected by the SolCyber SOC and are made available for 365 days before they are deleted from the system. SolCyber reserves the right to adjust fees if such logs collected are more than the logs considered normal for infrastructure of average verbosity.
2. *Alert Analysis and Triage* – SolCyber will analyze logs on a 24x7x365 basis for signs of malicious activity. Suspicious alerts will be triaged by SolCyber and escalated as an incident if confirmed.

3. *Incident Alerting* – Upon confirmation of an incident, SolCyber will create an incident in the SolCyber SOC and notify the Customer within the provided SLA.
4. *Portal Access* – Incidents will be made available via an online portal or other means at the discretion of SolCyber.

Endpoint Protection and Response Service

The SolCyber™ Endpoint Protection and Response ("**Endpoint Service**") provides protection against endpoint threats including threat detection, remote response and remediation assistance. The Endpoint Service is powered by a bundled endpoint solution.

Coverage: Endpoint protection and endpoint detection and response ("**EDR**") technologies approved and supported by SolCyber. An endpoint is defined as a laptop, workstation, desktop, server or virtual host at the End Customer environment.

Endpoint Licenses: Licenses will be provided by the Customer for technologies approved and supported by SolCyber.

1. *Policy Configuration and Management* – SolCyber will update EDR's configurations based off best practices and input from the Customer including device blocking.
2. *Response* – SolCyber will connect to confirmed incidents by remotely connecting to endpoints with EDR to perform additional triage, containment and response work when possible.
3. *EDR Troubleshooting* – SolCyber will respond to requests to troubleshoot issues related to EDR within the provided SLA.
4. *System Availability* – SolCyber will undertake reasonable measures to ensure that the EDR availability meets or exceeds the provided SLA.
5. *Performance and Availability Monitoring* – The EDR will be monitored 24x7x365 for anomalies in performance or availability. Upon confirmation of a fault, SolCyber will create an incident in the SolCyber SOC and notify the Customer within 4 hours.

2. Customer Responsibilities

In order to onboard the IRM Service, the Customer will need to be responsible for the following:

1. Manage all End Customer interactions and program management related tasks during the incident response engagement
2. Provide EDR license, setup the EDR tenant and register the licenses.
3. Assist End Customer to deploy the EDR:
    a. Provide EDR installation package

   b. Installation support and troubleshooting
   c. Provide monitoring for the first 24 hours until the hand-off to SolCyber
   d. Provide deployment status and alert updates to End Customer

4. Provide escalation contacts
5. Assist in transition of EDR tenant to SolCyber if the End Customer purchases Foundational Coverage service after the IRM service is complete

3. **Service Levels Agreement**

The purpose of this section is to describe the relevant actions, expectations, remedies, and exclusions related to the performance of Foundational Service. The Service Level Agreement ("SLA") is as follows:

SolCyber SOC SLA

SLA	Item	What It Is	Target Uptime
1	SOC Availability	Percent of minutes in a 1-month period	>=99.5%

The following definitions apply to this SLA:

- *"Downtime"* means Customer is not able to log in to SolCyber SOC and view a incident.
- *"Monthly Uptime Percentage"* means total number of minutes in a month (calculated as number of days in the applicable month x 24 hours x 60 minutes), minus the number of minutes suffered from Downtime in a month, divided by the total number of minutes in the month excluding periods of Planned Maintenance (Excused Downtime).
- *"Planned Maintenance"* will not count against Uptime and means any unavailability, suspension or termination to the extent caused by: (i) factors outside of SolCyber's reasonable control, including any force majeure event or Internet access or related problems beyond the demarcation point of SolCyber; (ii) any actions or inactions of Customer or any third party; (iii) SolCyber's suspension and/or termination of Customer's right to use the Service; (iv) any planned downtime or maintenance that SolCyber or its authorized service providers performs on the Service, provided that (a) Customer is notified at least seven days in advance or (b) Customer has agreed to the date and time of such non-emergency maintenance; or (v) any periods of shutdown necessitated by emergency maintenance.

- SolCyber reserves the right to disable any Customer’s rules and/or require them to be tuned to maintain this SLA.

SLA	Item	What It Is	Response Time Target
2	Mean Time to Triage - Suspicious Entity SLA	SolCyber will create Security Incident Case in SolCyber SOC	within 3 hours of when a Critical/High Severity Suspicious Entity is created/triggered.
3	Mean Time to Escalate - Security Incident SLA	SolCyber will escalate Security Incident Cases to Customer	Within 1 hour after it is assigned an Impact level of Sev-1, and within 3 hours after it is assigned an Impact level of Sev-2 in SolCyber SOC.
4	Mean Time to Troubleshoot – Technical Support SLA	SolCyber will begin troubleshooting “Technical Support Cases”	Within 3 business hours (defined as 9am to 5pm Eastern Time). For issues reported after the business day, troubleshooting will begin the next business day.

Security Incident Cases are considered escalated when either SolCyber changes the status to “Escalated to Customer” in SolCyber SOC or when an equivalent case/incident/ticket is created and linked in Customer’s 3rd party case management system that is integrated with SolCyber SOC.

Exclusions from coverage under this SLA:

- Suspicious Entities generated by one or more newly published Detection rules are excluded from this SLA until 7 days after the rule is published in SolCyber SOC (“Rule Probationary Period”). During the Rule Probationary Period, Suspicious Entities generated by newly published rules will still be monitored, triaged and investigated.
- Suspicious Entities generated by any Customer rules created by Customer in SolCyber SOC
- Suspicious Entities discovered during any Rule Probationary Period by newly developed rules and analytical models that are triggered by retroactive scans of existing logs as far back as 31 days.

- Should a Connector fail, SLAs will not apply during the period when the Connector is unavailable.
- SLAs do not apply during maintenance windows or in the event of any Customer-caused service outage that prohibits or otherwise limits SolCyber from providing the Service, including, but not limited to, Customer misconduct, Custom rule execution that results in Downtime for SolCyber SOC, negligence, inaccurate or incomplete information, and modifications made to the Service, hardware, or software by Customers, their employees or third parties acting on behalf of Customer. Maintenance windows ("Planned Maintenance Windows") for SolCyber SOC will be limited to a maximum of four hours per week (7-day period) unless communicated in writing by SolCyber.
- SLAs do not apply in the event Customer does not fulfil and comply with responsibilities and conditions set forth in this IRM Services SOW.

SLA	Item	What It Is	Target Uptime
5	Security Portal & API Availability	Percent of hours in a rolling 12-month period	99.95%
6	Security Service Availability	Percent of hours in a rolling 12-month period that the security service is operational	99.95%

The following definitions apply to this SLA:

- Measurement of the above SLAs will occur on a rolling 12-month basis, at the end of each calendar month.
- "Uptime" availability will be measured as the aggregate number of minutes during a year in which the AEP Service was available divided by the total number of minutes in the year (calculated as 365 days x 24 hours x 60 minutes) excluding periods of Planned Maintenance (Excused Downtime).
- "Planned Maintenance" will not count against Uptime and means any unavailability, suspension or termination to the extent caused by: (i) factors outside of SolCyber's reasonable control, including any force majeure event or Internet access or related problems beyond the demarcation point of SolCyber; (ii) any actions or inactions of Customer or any third party; (iii) SolCyber's suspension and/or termination of Customer's right to use the AEP Service; (iv) any planned downtime or maintenance that SolCyber or its authorized service providers performs on the AEP Service, provided that (a) Customer is notified at least seven days in advance or (b) Customer

has agreed to the date and time of such non-emergency maintenance; or (v) any periods of shutdown necessitated by emergency maintenance.

SLA	Item	What It Is	Response Time Target
7	"Mean Time to Respond – EDR Troubleshooting"	SolCyber will respond to troubleshoot request from the Customer for the endpoint protection and endpoint detection and response technology	Within 4 business hours from receiving an approved request (support@solcyber.com or a ticket request) submitted to the SOC. If the request is received within 4 business hours of a 5pm Eastern Time SOC operations cut-off, then the response shall be considered timely if completed within the next business day

II. PRICING & PAYMENT TERMS

1. Fees:

SolCyber will invoice Customer in US Dollars based on a fixed fee for a stated and fixed level of resources according to the applicable order form. The Customer acknowledges and agrees that it is paying for a fixed consumption of resources provided by SolCyber, and there will not be any credit should the actual resources deployed be less than the contracted amount. However, should the Customer require additional licenses that exceed the amount contracted, then the Parties will discuss a mutually agreed to increase in the fixed fee for the engagement. Additionally, should the time period for IRM Service exceed the period noted in Section I above, then the Parties will discuss a mutually agreed to increase in the fixed fee for the engagement. SolCyber shall propose this new amount to the Customer for agreement, and it shall be documented in the form of an amendment or change order to the applicable order form.

2. **Expenses:**

The fees noted in Section II, Item 1 do not include any travel or other costs directly authorized by the Customer in advance in connection with the provision of services under this IRM Services SOW. Should the Customer authorize SolCyber in writing to incur such additional travel or other costs, then SolCyber shall include in the next monthly invoice such costs following their incurrence.

3. **Invoicing and Payment Terms:**

Unless otherwise provided in the applicable order form, invoicing shall occur on the first day of the IRM Services term. Unless otherwise provided in the applicable order form, all invoices are due within thirty (30) days of the invoice date.