MASTER SERVICES AGREEMENT

BETWEEN

CLIENT

AND

SUMMIT 7 SYSTEMS, LLC
ORGANIZED IN THE STATE OF DELAWARE,
UNITED STATES OF AMERICA

Version: 07012026

PROPRIETARY AND CONFIDENTIAL

INTRODUCTION

This Master Services Agreement ("MSA") is entered into between Summit 7 Systems, LLC ("Company") and the Client. This MSA, together with any Statement of Work ("SOW") executed by the Parties, constitutes the binding agreement between the Parties. All sales of Products and/or Services by the Company to the Client are expressly conditioned upon the Client's acceptance of and compliance with the terms of this MSA. By executing a SOW, or by accessing or using any of the Products or Services provided by the Company, the Client acknowledges and agrees to be bound by the terms of this MSA. This MSA shall become effective on the Effective Date and shall remain in full force and effect unless and until terminated in accordance with the terms herein.

Order of Precedence

This MSA constitutes the entire agreement and understanding between the Client and Seller for Items as described in Article 1.1 of this document. There are no agreements, understandings, conditions, or representations, oral or written, that are not embodied in this MSA or that have not been superseded by this contract. The Client and Company agree that in the event of an ambiguity or inconsistency between the documents comprising this contract, the documents will be given a descending order of precedence as follows:
Master Services Agreement (MSA)
Statement of Work (SOW)
Any clause that might become part of this contract by operation of law or treaty
Any resulting Purchase Order from Client to Company

Definitions

"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with a Party.
"Assumptions" means the explicit conditions, dependencies, and facts that both parties agree must be true for the Company to deliver project services as scoped (e.g., cost, timeline, staffing, deliverables) as set forth in a SOW.
"Business Day" means any day from Monday through Friday, excluding any day designated as a federal holiday by statute or executive order.
"Change Order" means any written agreement modifying a SOW.
"Charges" means all amounts payable by the Client under this Agreement, including, without limitation, recurring monthly price charges for rented or purchased equipment, and licensing price.
"Client" means the legal entity identified in any applicable SOW and whose authorized representative has executed such document.
"**Client Data**" means all information processed or stored through the Client's Environment by Client or on Client's behalf.
"Cybersecurity Event" means occurrence that results in actual or potential jeopardy to the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
"Default" means a material breach of this Agreement or a failure to perform a material obligation under a SOW that remains uncured after the applicable notice period.
"Deliverables" means deliverables associated with any development milestone as specified in a SOW.
"**Effective Date**" means either: (a) the date of the final signature on the MSA or (b) the date of the final signature of any SOW referencing or governed by this MSA
"Environment" means the combination of hardware, software, networks, cloud services, configurations, and other technology components used by the Client to support its business operations and that are within the scope of Services provided under this Agreement. "Environment" excludes personal devices not owned or administered by Client, unless expressly agreed to in writing.
"**EOL Products**" means any hardware or software that is no longer supported by the original Third Party or maintained under a manufacturer's warranty or maintenance contract (e.g., end-of-life or end-of-support products).

"Hours of Operation" means the hours the Services are made available by Company to Client as set forth in a SOW.
"Indemnified Claim" means an Infringement Claim or Third Party Claim, as said terms are defined in Section 9.
"Indemnified Party" means a Party or Affiliate having a right to defense and indemnification under this Agreement that desires such defense and indemnification.
"Indemnitor" means a Party obligated to provide defense and indemnification under this Agreement.
"Intellectual Property Rights" means all copyrights, patents, registered and unregistered design rights, trademarks and service marks and applications for any of the foregoing, together with all trade secrets, know- how, rights to confidence and other intellectual and industrial property rights, in all parts of the world and for the full term thereof, including all rights to renew the same, belonging to a Party or a Third Party.
"Offboarding" refers to the set of activities performed at the conclusion or termination of Services to disengage the Company from the Client's Environment in a secure, organized, and auditable manner. This may include the return or removal of Company-owned equipment, software, credentials, and tools; transfer of documentation and administrative access; export or retrieval of Client data; decommissioning of managed systems or accounts; and the closure of service-related obligations. Offboarding may also involve coordination with Third Parties and confirmation that contractual, technical, and security-related responsibilities have been fulfilled.
"Parties" means Company and Client collectively.
"Party" means either Company or Client individually.
"**Personal Information**" means information that identifies, relates to, describes, is reasonably capable of being associated with, could reasonably be used to infer information about, or could reasonably be linked, directly or indirectly, with an individual person or household, as defined by applicable data protection or privacy laws.
"Products" means hardware, software, or subscription-based cloud services provided by a Third Party and resold by Company to Client pursuant to an SOW.
"Service Desk" refers to the centralized point of contact through which the Client submits service requests, reports incidents, and obtains support related to the Services. The Service Desk is responsible for logging, tracking, triaging, and facilitating the resolution of issues in accordance with the applicable Service Level Agreement (SLA), and may also provide status updates, knowledge resources, and general technical assistance.
"Service Level Agreement" or **"SLA"** refers to the defined performance standards, including response times, resolution targets, and service availability metrics, that Company commits to meet in connection with the delivery of Services, as set forth in an applicable SOW.
"Service Request" refers to a formal request submitted by a user or an authorized representative via the Service Desk for information, assistance, access, provisioning, or a change that is unassociated with service interruptions or failures.
"**Services"** means the services to be provided by Company to Client pursuant to a SOW.
"Statement of Work" or **"SOW"** means a contractual document issued under the MSA that defines the specific services, deliverables, timelines, responsibilities, pricing, and performance requirements applicable to a particular engagement. Each SOW outlines the detailed scope of work to be performed by Company, the Client's obligations, acceptance criteria, project milestones, and any assumptions or dependencies necessary for successful delivery.
"Strategic Account Manager" means the Client's primary point of contact at Company as set forth in a SOW or as otherwise communicated by the Company from time to time.
"**Taxes**" means taxes, levies, duties, tariffs, or governmental charges of any kind, including without limitation, sales, use, value-added, goods and services, excise, gross receipts, import, export, and withholding taxes, and any other similar taxes or charges imposed by any governmental authority, whether federal, state, local, or foreign.
"Third Party" means any individual, entity, or organization other than the Parties to this Agreement, including but not limited to subcontractors, suppliers, service providers, licensors, consultants, and vendors engaged by either Party.

1. Services.
1.1 Service Types. Company shall provide the following as specified in an applicable SOW:
1.1.1 Managed Services: Ongoing, recurring subscription-based services.
1.1.2 Project Services: Discrete, non-recurring services.
1.1.3 Out of Scope (OOS) Services: Services not expressly defined in a SOW, including work involving unsupported technologies or non-standard configurations. OOS work requires a written Change Order.
1.1.4 Beta Services: Services provided pursuant to an Addendum to a Managed Services SOW.

1.2 Access. Client grants Company necessary access to the Environment to perform Services. Client warrants the Environment is properly licensed. Company is not obligated to support unlicensed or expired software.

2. Products.
2.1 Resale. Company acts as a reseller of Third Party Products. All Products are subject to the Third Party's standard terms and warranties. Company will reasonably facilitate Third Party support processes but provides no independent warranty for Third Party Products.
2.2 Risk of Loss. All Products are delivered FOB Origin.
2.3 Regulatory Compliance. Client shall be solely responsible for obtaining all licenses, permits, authorizations, and approvals required by any applicable governmental authority, whether domestic or foreign, in connection with the purchase, shipment, import, export, or use of the Products.

3. Invoicing and Payment.
3.1 Billing. Company will invoice Client based on the following methods specified in the applicable SOW: (a) Time and Materials; (b) Firm Fixed Price (milestone-based); or (c) Recurring Monthly (Managed Services). Managed Services charges are not prorated and are invoiced in arrears on or about the 15th of each month.
3.2 Payment. Company will be paid based on the terms and at the rates quoted in each Quote or SOW created under this Agreement. Each SOW will identify if it is a Firm Fixed Price, Time & Materials, or Monthly Managed Services engagement. Client agrees to pay Company any undisputed amounts within thirty (30) calendar days of the date of invoice. Invoices not rejected or partially rejected within 15 days after the date of invoice shall be deemed accepted. Interest on money due under an invoice will accrue at a monthly rate of the lesser of (a) one and one-half percent (1.50%); or (b) the maximum rate permitted by applicable law, compounded monthly, calculated on the outstanding principal balance plus any previously accrued but unpaid interest, from the date such payment was due until paid in full. Client agrees to pay for all cost of collection of past due invoices, including reasonable attorneys' fees. Additionally, in the event of non-payment of undisputed amounts when due, Company reserves the right to suspend Services, access to the Environment, or delivery of Products after providing five (5) Business Days' written notice, without such suspension constituting a Default or a breach of this Agreement.
3.3 Reimbursable Expenses. Travel costs and other reimbursable expenses incurred by Company in connection with the performance of Services shall be invoiced in addition to the Charges stated in the applicable SOW. Travel costs shall be charged at actual cost plus applicable per diem, and other reimbursable expenses not otherwise included in the Charges for the Services shall be invoiced at actual cost. All reimbursable expenses shall be estimated, where feasible, in the relevant SOW and must be supported by receipts or other reasonable documentation, unless otherwise agreed in writing. Reimbursement shall be due in accordance with the payment terms set forth in this Section 3.
3.4 Taxes. Unless otherwise specified, prices include all applicable federal, state, and local taxes, duties, tariffs, and similar fees imposed by any government, all of which shall be listed separately on the invoice.

4. Termination.
4.1 Effect of Early Termination. Company is entitled to receive the full amount it would have been paid if Client had not terminated the MSA or SOW early.
4.2 Termination for Default. Company or Client shall have the right to cancel this Contract partially or completely in the case of Default by the other party. Any cancellation will be effective if, written notice stipulating the nature of the breach is provided by the canceling party to the other party, and the breach is not cured within sixty (60) days of receipt of such notice.
4.2.1 Default by Company. If the MSA or SOW is canceled by Client for Default by Company, payments received by Company in excess of services or work performed, including allocable profit, will be refunded. In the event that the cost incurred by Company is greater than the advance payment, the Client shall be liable to Company for such amount. The above shall constitute the sole liability of Company and the exclusive remedy of the Client for Default by the Company.
4.2.2 Default by Client. If the MSA or SOW is canceled by Company for Default of Client, Company will have the right to be paid all Charges specified in the applicable SOWs, including allocable profit, for work or services performed up to the date of cancellation plus necessary termination expense for materials and services initiated.

5. Confidentiality.

5.1 Confidentiality Definition. Company and Client each wish to have access to certain materials and information of the other for the purpose of this Agreement for the acquisition of Products and Services. Both Parties considers its materials and information to be proprietary and is only willing to provide such materials and information to the other Party under the terms and conditions of this Agreement. For purposes of this Agreement, "Confidential Information" is defined as any non-public data that either Party or its representatives (the "Disclosing Party") provide to another party (the "Receiving Party"), whether disclosed in written, oral, electronic, or any other form, including but not limited to: (a) Technical data, designs, or intellectual property; (b) Business strategies, pricing, financial forecasts, customer lists, and other commercial information; (c) Software, documentation, prototypes, know-how, trade secrets, and system configurations; or (d) Information marked or otherwise designated as "Confidential" or that reasonably should be understood as confidential given its nature. Confidential Information will not include materials and information already in the public domain or known to the receiving Party (as evidenced by written records) when first received from the disclosing Party and Confidential Information will lose its status as Confidential Information if, and as of the date when, it becomes part of the public domain through no wrongful act of the receiving Party, is rightfully disclosed to the receiving Party without restriction by a source other than the disclosing Party, or is developed by the receiving Party entirely independently of any disclosure hereunder. Confidential Information disclosed under this Agreement is made without any representation, guarantee, or warranty of any kind. This Section 5 contains the entire understanding between the Parties regarding Confidential Information disclosed on or after the effective date of this Agreement and supersedes and replaces all prior Agreements.

5.2 Injunction. Recipient agrees that: (a) no adequate remedy exists at law if it breaches this Section 5; (b) it would be difficult to determine the damages resulting from such breach; (c) such breach would cause irreparable harm to Discloser; and (d) a grant of injunctive relief provides the best remedy for any such breach, without any requirement that Discloser prove actual damage or post a bond or other security. Recipient waives any opposition to such injunctive relief or any right to such proof, bond, or other security.

5.3 Termination & Return. The confidentiality obligations in this Section 5 will survive the termination of this Agreement. Upon termination of this Agreement, Recipient shall return all copies of Confidential Information to Discloser or certify, in writing, the destruction thereof; except that each Party may retain an archived copy to be used only in case of a dispute arising under an Agreement, and in such case only to the extent disclosure is reasonably necessary in connection with any dispute, claim, or action between the Parties. Notwithstanding the foregoing, the obligations to return or destroy Confidential Information shall not cover information that is maintained on routine computer system back-up storage devices; in each case so long as retained or backed up information is kept confidential in accordance with the confidentiality obligations hereunder.

5.4 Retention of Rights. This Agreement does not transfer ownership of Confidential Information or grant a license thereto. Except to the extent another section of this Agreement specifically provides to the contrary, Discloser will retain all right, title, and interest in and to all Confidential Information. Neither Party shall reverse engineer, reverse translate, disassemble or decompile any computer programs, appliances, prototypes or other tangible objects that embody the other Party's Confidential Information or that are provided to the Party under an Agreement.

5.6 Feedback. If Client or its personnel provide any suggestions, ideas, or other feedback related to Company's products or services ("Feedback"), Company may use such Feedback for any lawful purpose, including improving or developing its offerings, without obligation to compensate or credit Client. Company's rights under this Section apply only to Feedback that does **not** include Client's Confidential Information. Client may not designate Feedback as Confidential Information if the Feedback relates solely to Company's products, services, or business operations. Any portion of Feedback that includes or is inseparable from Client's Confidential Information will remain protected under this Agreement, and Company will not use that portion except as permitted for Confidential Information.

5.7 Monitoring. Company may monitor and collect configuration, performance, and usage data relating to Client's use of the Products and Services (a) to facilitate delivery of the Products and Services; and (b) improve delivery of the Products and Services. Client shall not interfere with such monitoring.

6. Data Management, Privacy, and Security

6.1 Security Measures. Company maintains commercially reasonable administrative, technical, and physical safeguards to protect the security and privacy of Client Data. Company's systems and processes are designed to comply with the Cybersecurity Maturity Model Certification (CMMC) framework, and Company undergoes regular

audits and assessments to verify ongoing compliance with CMMC requirements. Certain Services may also be designed to support Client's compliance with additional security standards or regulatory frameworks, as expressly set forth in the applicable SOW. While Company may support Client's compliance efforts through these Services, Company does not guarantee Client's compliance with any specific law, regulation, or standard. Client acknowledges and agrees that the transmission, storage, and processing of data over the internet involves inherent risks of unauthorized access, disclosure, or exposure. By accessing and using the Environment, Products, and Services, Client assumes such risks. Except as expressly stated in a SOW, Company makes no representation or warranty that the Products or Services will ensure Client's compliance with any particular regulatory or industry requirement. Notwithstanding anything to the contrary herein, Company does not guarantee, and expressly disclaims, security or compliance with any data security standards in connection with the use of hardware or software that is no longer supported by the original Third Party (e.g., end-of-life or end-of-support products) ("EOL Products"). Client assumes full responsibility for the use of any EOL Products, including any resulting security vulnerabilities, non-compliance, or data exposure, and agrees that Company shall have no liability arising from or related to such use.

6.2 Audits. Company will conduct an audit of its security measures and Client shall have such audit rights as set forth in the Data Processing Addendum ("DPA" or "Addendum") attached hereto as Exhibit A.

6.3 Data Processing and Access Control. The Parties agree to the terms of the Data Processing Addendum attached as Exhibit A and the Access Control Policy attached as Exhibit B, each of which is hereby incorporated into this Agreement by reference.

6.4. Client Responsibilities.

6.4.1 Client Data. Client is solely responsible for implementing appropriate administrative, technical, and physical safeguards for Client Data. If Client requires Company to meet data protection, cybersecurity, or regulatory obligations beyond those stated in this Agreement, Client must provide written notice; any such requirements may involve additional terms or Charges. Client is responsible for determining the suitability of the Product or Service for its data and intended use. Company does not provide data hosting, storage, or archiving services and will not retain Client Data more than thirty (30) days after Service termination, after which such data may be deleted. Except as expressly provided in this Agreement, Company will not restore or deliver Client Data related to terminated Services, and Client is responsible for migrating its data within the thirty (30) day post-termination period. Except as required by law, all breach-notification obligations relating to Client Data are solely the Client's responsibility and cost.

6.4.2 Acceptable Use. Client remains solely responsible for the actions and omissions of its users in connection with their access to and use of Client's Environment and any Services. Client agrees, and shall ensure its users agree, to use the Environment and the Services in a lawful and responsible manner. Without limitation, Client and its users shall not engage in any activity that is unlawful, abusive, or disruptive in connection with their use of the System, including but not limited to: hacking, phishing, spamming, identity theft, financial fraud, e-mail spoofing, malware distribution, denial-of-service attacks, unauthorized access to data or systems, infringement of Intellectual Property Rights, distribution of pirated or illegal software, or harassment. Furthermore, Client shall not utilize artificial intelligence (AI), machine learning (ML), or large language models (LLMs) in a manner that permits the input of Client Data, particularly Controlled Unclassified Information (CUI) or Personal Information (PII), into any third-party or public AI service that has not been explicitly approved in a SOW and verified to meet the security and compliance standards required by this Agreement. Company may investigate any suspected violation of this Section 6.4.2. If Company determines that a violation has occurred, it may, in its sole discretion and without limiting any of its other rights or remedies: (a) restrict Client's and its users' access to the Services; (b) remove or require removal or remediation of any content, code, or activity believed to be in violation; (c) suspend or limit its support of the affected systems; (d) terminate this Agreement for cause; and/or (e) pursue any other remedies available at law or in equity. Except in cases of emergency or where otherwise required by applicable law, Company will make reasonable efforts to notify Client of any enforcement action taken under this Section 6.4.2 using commercially reasonable means, such as telephone or email. Client shall promptly notify Company of any actual or suspected security incident, policy violation, or other circumstance involving its users or the Environment that may affect the Services or result in a claim against Company. Client agrees to cooperate with Company by providing relevant information upon request in connection with any such event. Company agrees to provide Client with reasonable access to Client's software applications, devices, and equipment, and to any license or configuration files related to the Services, to the extent such access is required for Client to verify user compliance with the terms of this Agreement and does not compromise the integrity or security of Company's systems, Third Party tools, or confidentiality obligations to Third Parties.

6.4.3 Encryption. Client shall implement application-level encryption for all Information and data that is considered sensitive, confidential, or otherwise subject to protection under applicable U.S. federal or state law, foreign or international data protection regulations, or Client's contractual obligations to Third Parties. Client is solely responsible for ensuring that encryption is implemented in a manner consistent with applicable standards and regulatory requirements, including but not limited to NIST, ISO/IEC 27001, FIPS 140-2, or other industry-accepted encryption benchmarks, as applicable to the nature and jurisdiction of the data.

6.5 Cybersecurity Event. The Party affected by a Cybersecurity Event shall use commercially reasonable efforts to mitigate the impact thereof and to resume performance as soon as reasonably practicable; provided however, that should any delay or failure continue for more than ten (10) Business Days, the Agreement may be terminated without liability by the non-affected Party. Notwithstanding the foregoing, Company shall not be deemed in breach for suspending or limiting Services to protect against or respond to cybersecurity threats or incidents.

7. Warranties.

7.1 Mutual Warranties. Each Party warrants to the other Party that: (i) it has full corporate right, power, and authority to enter into, execute, and perform its obligations under this Agreement; (ii) the performance of its duties and obligations hereunder do not and will not violate any agreement or other legal obligation by which it is bound; and (iii) it is, and will continue to be, in material compliance with all laws and regulations applicable to its performance of, or obligations under, this Agreement, including in its provision or use of the Products and Services. Each Party further acknowledges and agrees that it shall be solely responsible for complying with such applicable laws and regulations in connection with its respective obligations under this Agreement.

7.2 Company Warranties. Company warrants that the Company and any Company Affiliates assigned to perform the Services will perform the Services in material conformance with the terms of the applicable SOW during the term thereof. Company further warrants that Company and any Company Affiliates assigned to perform the Services are qualified to perform their assigned tasks. Client's sole and exclusive remedy for breach of this warranty will be, at Company's sole option (a) re-performance of the nonconforming Services materially as described in the applicable Agreement; or (b) a pro rata refund of fees previously paid to Company for the nonconforming Services. For Services containing Deliverables, such Services will be deemed accepted by Client if not rejected in a reasonable detailed writing within five (5) calendar days of submission of the Deliverable to Client, or as otherwise identified in an applicable SOW. In the event such Services provided by Company are not in conformance with this warranty, Client must provide written notice to Company within such period and such notice will specify in reasonable detail the nature of the deficiency. Notwithstanding anything to the contrary herein, Company provides no warranty, and will have no responsibility for, any claim arising out of (a) modification of the Products or Services by anyone other than Company; (b) use of the Products or Services in combination with any operating system, hardware, or software not authorized in the SOW; (c) damage to the Products or Services by Client, including without limitation through misapplication, misuse, abuse, accident, neglect, or mishandling; (d) the performance of the Services after the expiration or earlier termination of the applicable SOW; or (e) the acts or omissions of Client. Client acknowledges and agrees that any Products provided by Company are manufactured, licensed, or otherwise supplied by a Third Party and are subject exclusively to the terms, conditions, representations, and warranties, if any, provided by the applicable Third Party or manufacturer. Client is not authorized to make, and Client shall not make any representations or warranties on behalf of Company to any Third Party. Client shall be solely responsible and liable for any representations or warranties that Client makes to any Third Party regarding Company, the Products, Services, or any other aspect of this Agreement.

7.3 Client Warranties. Client is solely responsible for the accuracy, legality, and appropriateness of all Client Data. Client represents and warrants that Client Data will not: (a) infringe any intellectual property, privacy, confidentiality, or publicity rights; (b) contain illegal, harmful, or prohibited content, including viruses or malicious code; (c) violate laws governing unsolicited communications; (d) create risk of harm or liability; (e) include material Client lacks the right to use; (f) violate any law or this Agreement; (g) contain classified information, CUI, FCI, or other restricted data unless expressly authorized in a SOW and supported by compliant systems; or (h) contain any prohibited data. Additionally, to the extent Client Data is generated, modified, or processed using artificial intelligence (AI), machine learning (ML), or large language models (LLMs), Client represents and warrants that: (a) such data is accurate, complete, and meets the integrity standards required for the Services; (b) the use of such AI tools has not resulted in the loss of necessary metadata or the improper reclassification of sensitive information, including CUI or PII; and (c) such data does not infringe upon the Intellectual Property Rights of any Third Party. Finally, Client warrants it has

all rights and consents required to provide Client Data to Company and to permit Company to process it as described in this Agreement. Client is solely responsible for compliance with all applicable federal laws and regulations governing data classification, access, and handling, including FAR, DFARS, ITAR, and NISP. Company is not liable for any loss, damage, or exposure resulting from Client's non-compliance or unauthorized use of the Products or Services.

7.4 Service Levels. Notwithstanding anything to the contrary herein, for Services with technical standards of performance or service levels, if any, set forth in the applicable SOW, Client's sole and exclusive remedy for any failure to meet such applicable technical standards of performance or service levels shall be as specified in the applicable SOW.

7.5 Compliance. Company provides advisory and support services designed to assist Clients in aligning with the requirements of the Cybersecurity Maturity Model Certification (CMMC) framework. These services are consultative in nature and do not constitute a certification, audit, or official assessment under the CMMC program. Company does not guarantee or warrant that the Client will achieve a specific outcome. Certification decisions are solely the responsibility of a Department of Defense (DoD)-authorized Certified Third Party Assessment Organization (C3PAO) or the appropriate government authority. While Company may be responsible for implementing, partially implementing, or advising Client on implementation of controls, processes and practices, the Client maintains accountability and authority for client's cybersecurity and compliance program.

8. EXCLUSION OF LIABILITIES

8.1 DISCLAIMER AND RELEASE. THE WARRANTIES, CONDITIONS, REPRESENTATIONS, OBLIGATIONS AND LIABILITIES OF COMPANY AND REMEDIES OF CLIENT SET FORTH IN THIS AGREEMENT ARE EXCLUSIVE AND IN SUBSTITUTION FOR, AND CLIENT HEREBY WAIVES, RELEASES AND RENOUNCES ALL OTHER WARRANTIES AND OTHER OBLIGATIONS AND LIABILITIES OF COMPANY, AND ANY OTHER RIGHTS, CLAIMS AND REMEDIES OF CLIENT AGAINST COMPANY, EXPRESS OR IMPLIED, ARISING BY LAW OR OTHERWISE, WITH RESPECT TO ANY NONCONFORMANCE OR DEFECT IN ANY ITEMS OR OTHER THINGS PROVIDED UNDER THIS AGREEMENT, INCLUDING BUT NOT LIMITED TO: A) ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS; B) ANY IMPLIED WARRANTY ARISING FROM COURSE OF PERFORMANCE, COURSE OF DEALING OR USAGE OF TRADE; C) ANY OBLIGATION, LIABILITY, RIGHT, CLAIM OR REMEDY IN TORT, WHETHER OR NOT ARISING FROM THE NEGLIGENCE OF COMPANY; AND D) ANY OBLIGATION, LIABILITY, RIGHT, CLAIM OR REMEDY FOR LOSS OF OR DAMAGE TO ANY PROPERTY OF CLIENT, INCLUDING WITHOUT LIMITATION ANY ITEMS.

8.2 EXCLUSION OF CONSEQUENTIAL AND OTHER DAMAGES. COMPANY SHALL HAVE NO OBLIGATION OR LIABILITY, WHETHER ARISING IN CONTRACT (INCLUDING WARRANTY), TORT (WHETHER OR NOT ARISING FROM THE NEGLIGENCE OF COMPANY), OR OTHERWISE, FOR LOSS OF USE, REVENUE OR PROFIT, OR FOR ANY OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES WITH RESPECT TO ANY NONCONFORMANCE OR DEFECT IN ANY ITEMS OR OTHER THINGS PROVIDED UNDER THIS AGREEMENT.

8.3 LIMITATION OF LIABILITY. NOTWITHSTANDING ANYTHING TO THE CONTRARY, COMPANY'S TOTAL AGGREGATE LIABILITY FOR ALL CLAIMS ARISING OUT OF THIS AGREEMENT SHALL NOT EXCEED THE GREATER OF: (A) THE TOTAL CHARGES PAID BY CLIENT TO COMPANY IN THE SIX (6) MONTHS PRECEDING THE EVENT GIVING RISE TO THE CLAIM; OR (B) THE TOTAL CHARGES PAID BY CLIENT UNDER THE APPLICABLE SOW DURING THE TWELVE (12) MONTHS PRECEDING THE EVENT.

9. Indemnification.

9.1 Indemnification by Client. Client shall indemnify, defend, and hold harmless **Company**, including its subsidiaries, Affiliates, subcontractors, suppliers, and their respective directors, officers, employees, and agents, from and against any and all claims, damages, losses, liabilities, penalties, judgments, costs, and expenses (including reasonable attorneys' fees) arising out of or related to: a) Client's misuse or unauthorized use of any Company services, deliverables, software, or materials; b) Client's failure to comply with applicable laws, regulations, or contractual obligations; c) any claim alleging that data, content, or materials provided by Client infringes, misappropriates, or otherwise violates the rights of any Third Party; d) any negligent, reckless, or intentional act or omission by Client or its personnel; and e) any security incident, data breach, or unauthorized access arising from Client's systems, environments, credentials, or actions.

9.2 Indemnification by Company. Company shall indemnify, defend, and hold harmless Client from and against Third Party claims to the extent directly arising out of Company's gross negligence or willful misconduct in the performance

of services under this Agreement. This indemnification obligation is subject to, and limited by, the Exclusion of Liabilities set forth in Section 8 of this Agreement.

9.3 Conditions of Indemnification. The indemnifying party's obligations under this Section are conditioned upon the Indemnified Party: a) providing prompt written notice of any claim for which indemnification is sought; b) granting the Indemnifying Party sole control over the defense and settlement of the claim, provided that any settlement binds the Indemnified Party only if it contains no admission of wrongdoing and imposes no obligations beyond monetary payment; and c) providing reasonable cooperation, at the indemnifying party's expense, in the defense of such claim.

9.4 Sole Remedy. Except as otherwise expressly provided in this Agreement, the indemnification obligations in this Section constitute the **sole and exclusive remedy** of the Indemnified Party for the claims described herein.

9.5 Procedure for Claims. The Indemnified Party shall provide prompt notice of any Indemnified Claim to Indemnitor and reasonably cooperate with Indemnitor's defense. Indemnitor will control the defense of any Indemnified Claim, including appeals, negotiations, and any settlement or compromise thereof; provided: (a) if Indemnitor fails to assume the defense on time to avoid prejudicing the defense, Indemnified Party may defend the Indemnified Claim, without loss of rights pursuant to this Section 9, until Indemnitor assumes the defense; and (b) Indemnified Party will have the right, not to be exercised unreasonably, to reject any settlement or compromise that requires that it or any indemnified Affiliate admit wrongdoing or liability or subjects either of them to any ongoing affirmative obligation. Indemnitor's obligations above in this Section 9 will be excused if either of the following materially prejudices the defense: (i) Indemnified Party's failure to provide prompt notice of the Indemnified Claim; or (ii) Indemnified Party's or an Affiliate's failure reasonably to cooperate in the defense of an Indemnified Claim.

10. Insurance. During the term of this Agreement, each Party shall, at its own expense, maintain insurance coverage from a reputable insurer. For the avoidance of doubt, each Party is solely responsible for insuring its own property, regardless of location, and acknowledges that the other Party shall have no obligation to insure, or liability for loss of, such property while in transit or in the possession or control of the other Party.

11. Ownership Rights.

11.1 Client Data. As between the parties, Client retains all right, title, and interest in and to Client Data, including any and all Intellectual Property Rights therein. Company's access to and use of Client Data is solely on Client's behalf and for the limited purposes described in this Agreement. Nothing in this Agreement shall be construed to grant Company any ownership rights in or to Client Data. Client hereby grants to Company a non-exclusive, non-transferable (except pursuant to a permitted assignment), royalty-free license to use, store, transmit, copy, display, process, delete, retain, and modify Client Data solely to perform the Services, fulfill or enforce contractual obligations, comply with applicable law, regulation, legal process, or government request, maintain, secure, support, and improve the Services, and generate statistical, analytical, and other aggregated, non-personally identifiable data.

11.2 Services. Except as otherwise expressly provided in an applicable SOW or in Section 11.3, Client acknowledges that as between Client and Company, all Intellectual Property Rights in the Services, and any and all improvements, enhancements, modifications, or derivative works thereof, whether or not made at Client's request, are and shall belong to and remain the property of Company as they pertain to the Services. No creation of or modifications to the Services by Company pursuant to Client's request shall be considered as consulting, producing, or resulting in a "work for hire" under the copyright laws of the United States. Company shall for all purposes be deemed the author and originator of all Services directly resulting from any work performed by Company pursuant to this Agreement.

11.3 Deliverables. Subject to the terms of the applicable SOW and upon payment in full of all fees associated with such Deliverable, all Deliverables specifically identified as such in an SOW shall be owned by Client. To the extent such Deliverables are deemed "work made for hire" under applicable law, they shall be owned by Client; to the extent they do not qualify as such, Company hereby assigns all right, title, and interest in such Deliverables to Client. Notwithstanding the foregoing, Company retains all right, title, and interest in and to its Services, its pre-existing intellectual property, and any improvements, enhancements, or derivative works of its Services made during the performance of the SOW, regardless of whether such improvements were requested by Client.

12. Dispute Resolution.

12.1. Negotiation. The parties shall attempt in good faith to resolve any dispute arising under this Agreement through direct discussions between their designated representatives. If not resolved within **10 Business Days**, the dispute shall be escalated to senior executives, who will attempt to resolve it within **15 Business Days**.

12.2. Mediation. If the dispute remains unresolved, either party may request non-binding mediation in **Madison County, Alabama,** under the **AAA Commercial Mediation Procedures**. The parties will share the mediator's fees equally.
12.3. Arbitration. If mediation does not resolve the dispute within **30 days**, the matter shall be finally settled by **binding arbitration** in **Madison County, Alabama,** under the **AAA Commercial Arbitration Rules** before a single arbitrator. The arbitrator's award shall be final and enforceable in any court of competent jurisdiction, and may include reasonable attorneys' fees and costs.
12.4. Injunctive Relief. Either party may seek temporary or preliminary injunctive relief in a Delaware court to prevent immediate and irreparable harm, without waiving the obligation to arbitrate all other issues.

13. Additional Terms.
13.1 Governing Law and Venue. This Agreement is governed by Delaware law. The parties submit to the exclusive jurisdiction of the courts in Madison County, Alabama, and Company may bring actions in such courts to collect undisputed amounts owed it by Client.
13.2 Notices. All notices, requests, consents, and other communications required or permitted under this Agreement shall be in writing and shall be deemed properly given when delivered to the receiving Party at the address set forth in this Agreement (or to such other address as a Party may designate in writing), and delivered by one of the following methods: (a) certified or registered mail (return receipt requested); (b) nationally recognized overnight courier service; (c) electronic mail subject to the conditions below; or (d) personal delivery. Notices shall be deemed effective: (i) on the date received, as evidenced by the return receipt, courier tracking record, or signed delivery confirmation, for notices sent by mail, courier, or personal delivery; and (ii) on the date of successful transmission for notices sent by electronic mail, provided that no bounce-back, delivery failure, or other error message is received. All notices to Company delivered by electronic mail must be sent to: **Contracts@summit7.us**. Email notices sent to any other address will not be deemed valid.
13.3 Force Majeure. No delay, failure, or Default, other than a failure to pay Charges when due when payment can still be made electronically or through other means, will constitute a breach of this Agreement to the extent such delay, failure, or Default results from a Force Majeure Event. The Party affected by a Force Majeure Event shall use commercially reasonable efforts to mitigate the impact thereof and to resume performance as soon as reasonably practicable; provided however, that should any delay or failure continue for more than thirty (30) days, the Agreement may be terminated without liability by the non-affected Party. Notwithstanding the foregoing, Company shall not be deemed in breach for suspending or limiting Services to protect against or respond to cybersecurity threats or incidents.
13.4 Severability. To the extent permitted by applicable law, the Parties hereby waive any provision of law that would render any provision or clause of this Agreement invalid or otherwise unenforceable in any respect. If any provision of this Agreement is adjudged invalid, illegal, or unenforceable by a court of competent jurisdiction, or is invalid by operation of any applicable law, such provision will be interpreted to achieve its original effect to the maximum extent permitted by applicable law, and the remaining provisions will continue in full force and effect.
13.5 Waiver. No failure or delay by either Party in exercising any right, power, or remedy under this Agreement will operate as a waiver. No waiver will be effective unless it is in writing signed by an authorized representative of the waiving Party. No waiver of a breach of this Agreement will constitute a waiver of any other breach of this Agreement.
13.6. Survival. The provisions of this Agreement which by their nature should survive termination or expiration shall so survive, including but not limited to: Sections concerning payment obligations, confidentiality, Intellectual Property Rights, limitations of liability, indemnification, dispute resolution, data management and security, governing law, and any other provisions necessary to enforce or interpret the Parties' rights and obligations following termination.
13.7. Assignment. Neither Party may assign this Agreement, in whole or in part, without the other Party's prior written consent; provided, however, that either Party may assign this Agreement to an acquirer of all or substantially all its stock or assets. Any other attempt to assign this Agreement without such consent will be null and void. Notwithstanding the foregoing, Client expressly acknowledges that Company may engage contractors to contribute to or assist with Company's obligations under this Agreement, and Client expressly agrees that such engagement of contractors is permitted and will not constitute an assignment.
13.8. Publicity. Except as expressly provided herein, neither Party shall issue any public announcement, press

release, or other publicity regarding the existence or terms of this Agreement, or the nature of the Services provided, without the prior written consent of the other Party. Notwithstanding the foregoing, Company may use Client's name and logo on its web site, in its marketing materials, and in presentations solely to identify Client as a customer, provided that such use is in accordance with any brand usage guidelines provided by Client and does not suggest endorsement. Client may revoke this permission at any time upon written notice to Company, at which point Company shall promptly cease further use.

13.9. Amendment. Company may amend this Agreement from time to time with respect to general, administrative, or non-material provisions, including but not limited to updates to product or service descriptions, technical documentation, compliance-related policies, or branding, by releasing it to Client in writing. Company may amend this Agreement as reasonably necessary to comply with changes in applicable laws, regulations, or governmental requirements. Such amendments will become effective thirty (30) days after release.

13.10 Non-Solicitation. During the term of this Agreement and for a period of twelve (12) months thereafter, Client shall not, directly or indirectly, solicit for employment, hire, or engage as an independent contractor any employee or contractor of Company who was involved in the performance of Services under this Agreement, without Company's prior written consent. In the event of a breach of this Section, Client agrees to pay Company a placement fee equal to 100 percent of the individual's new annual gross salary.

EXHIBIT A

DATA PROCESSING ADDENDUM

1. DEFINITIONS
All capitalized terms not otherwise defined herein shall have the meanings given in the MSA.

"Applicable Data Protection Laws" means all data protection, privacy, and cybersecurity laws and regulations of the United States applicable to the processing of Personal Data under the Agreement, including, where applicable: the California Consumer Privacy Act of 2018 (as amended by the California Privacy Rights Act) ("CCPA"), the Virginia Consumer Data Protection Act ("VCDPA"), the Colorado Privacy Act ("CPA"), the Utah Consumer Privacy Act ("UCPA"), and other similar U.S. state privacy laws; and, where applicable, the Federal Information Security Modernization Act ("FISMA"), Defense Federal Acquisition Regulation Supplement ("DFARS") 252.204-7012, the Cybersecurity Maturity Model Certification ("CMMC"), National Institute of Standards and Technology Special Publication 800-171 ("NIST SP 800-171"), and other federal regulations concerning Controlled Unclassified Information ("CUI").
"Client Data" means all data, including Personal Data and/or Controlled Unclassified Information (CUI), provided to Company by or on behalf of Client in connection with the Services under the Agreement.
"Controlled Unclassified Information (CUI)" has the meaning assigned in 32 C.F.R. Part 2002 and DFARS 252.204-7012 and refers to unclassified information that requires safeguarding or dissemination controls pursuant to law, regulation, or government-wide policy.
"Personal Data" means any Personal Information relating to an identified or identifiable individual or household, as defined under Applicable Data Protection Laws that Client submits or otherwise sends to the Client's Environment or the Services.
"Personal Data Incident" means a confirmed breach of security of the Services leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data in Company's possession and control.
"Processing" or **"Process"** means any operation performed on Client Data, including collection, storage, use, access, disclosure, or deletion.
"Sub-processor" means any third party engaged by Company to Process Client Data on its behalf under the Agreement.
"Data Subject" means a natural person or household to whom Personal Data relates.

2. PURPOSE AND SCOPE: This Addendum applies only to the extent Company Processes Personal Data on behalf of Client in connection with the Agreement. The Parties agree that Client is the data controller or business with respect to Client Data, and Company is the processor or service provider, processing Client Data solely on Client's behalf.
(a) Scope of Personal Data and Data Subjects. The types of Personal Data and the categories of Data Subjects under the Agreement and this DPA are set forth in Appendix 1 of this Addendum. Company shall not be responsible for Processing any Personal Data not identified in Appendix I. If Client uses the Products or Services to process any categories of Personal Data not expressly covered by this Addendum, Client acts at own risk and Company shall not be responsible for any compliance deficits related to such use. Client is responsible for providing all notices and obtaining all consents required by Applicable Data Protection Laws for Company's Processing of Personal Data.
(b) Compliance with Applicable Law. Client shall in its use of the Services, comply with its obligations under Applicable Data Protection Laws in its Processing of Personal Data and any Processing instructions it issues to Company. Company shall Process Client Data solely to perform its obligations under the Agreement and in accordance with Client's documented instructions.
(c) Scope of Processing Instructions and **Limitations.** Client agrees that the Agreement is its complete and final instructions to Company in relation to the Processing of Personal Data. Processing any Personal Data outside the scope of the Agreement will require prior written agreement between Company and Client by way of an amendment to the Agreement and will include any additional Charges that may be payable by Client to Company for carrying out such instructions.

3. SUB-PROCESSING:

(a) Use of Sub-Processors. Client gives Company a general authorization to engage Sub-Processors in connection with the provision of the Services provided that (i) Company maintains a list of current Sub-Processors; (ii) Sub-Processors are bound by written agreements that provides for, in substance, the same data protection obligations as those binding Company under this DPA, to the extent applicable to the services provided by the Sub-Processor; and (iii) Company remains liable for Sub-Processor's actions.
(b) New Sub-Processors. A list of Company's current Sub-Processors is available upon request. Client hereby consents to these Sub-Processors, their locations, and their processing activities. Company will notify Client of changes to Sub-Processors and provide an opportunity to object. If Client has a reasonable objection to a new Sub-Processor and provides it in writing to Company within 30 days of such notice, Company will use reasonable efforts to make available to Client a change in the Services or a reasonable change to Client's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-Processor, provided that if the objection relates to a major infrastructure provider (e.g., Cloud Service Provider), Company shall not be required to replace such provider, and Client's sole remedy shall be termination of the affected SOW.

4. SECURITY MEASURES: Company shall maintain appropriate administrative, technical, and physical safeguards to protect Personal Data in accordance with Appendix II. Company shall ensure personnel authorized to access Personal Data are subject to confidentiality obligations. Company shall notify Client of a Personal Data Incident without undue delay and in accordance with the Agreement.

5. DELETION OF DATA: Client hereby elects that following the termination or expiration of the Agreement Company shall delete all Personal Data in Company's possession and control as provided in the Agreement, except to the extent Company is required by applicable law to retain some or all of the Personal Data (in which case Company will archive the data and implement reasonable measures to prevent the Personal Data from any further Processing, and the terms of this DPA will continue to apply to such Personal Data.

6. PERSONAL DATA INCIDENT RESPONSE: Company will notify Client without undue delay and in accordance with applicable laws after becoming aware of a Personal Data Incident. Company will make reasonable efforts to identify the cause of the Personal Data Incident and take such steps as Company deems necessary and reasonable in order to remediate the cause of such a Personal Data Incident to the extent the remediation is within Company's reasonable control. Company will provide information relating to the Personal Data Incident as reasonably requested by Client. The obligations herein shall not apply to incidents that are caused by Client, its employees, subcontractors, customers, or users.

7. AUDIT REPORTS: Company obtains Third Party audits of its compliance against data protection and information security standards on a regular basis ("Audits"). Upon Client's written request and subject to obligations of confidentiality, Company may make available to Client a summary of its most recent Audits, and/or other documentation so that Client can verify Company's compliance with this DPA.

8. DATA TRANSFERS: Company may transfer Personal Data to and Process Personal Data in the United States where Company or its Sub-Processors maintain data processing operations as necessary to provide the Services. Company shall not transfer Client Data outside the United States without Client's prior written consent, unless required by applicable law.

9. DATA SUBJECT REQUIREMENTS:
(a) Subject Access Requests. If Company receives any requests from Data Subjects relating to the Processing of Personal Data under the Agreement, Company will promptly redirect the request to the Client to the extent legally permitted. Client authorizes Company to respond to such Data Subjects to confirm that Company has redirected the request to Client; otherwise, Company will not respond to such communication directly without Client's prior authorization, unless legally required to do so. If Company is legally required to respond to such a request, Company will promptly notify Client and provide Client with a copy of the request, unless legally prohibited from doing so.
(b) Assistance. Company will reasonably cooperate with Client, at Client's expense, to permit Client to respond to any requests from Data Subjects or applicable data protection authorities relating to the Processing of Personal Data under the Agreement taking into account the nature of the Processing, and to the extent that Client is unable to

access the relevant Personal Data in its use of the Services.

(c) DPIAs and Prior Consultations. To the extent required by Applicable Data Protection Laws, Company will, upon reasonable notice and at Client's expense, provide reasonably requested information regarding the Services to enable Client to carry out data protection impact assessments ("DPIAs") and/or prior consultations with data protection authorities.

10. CHANGES IN LAW: The parties shall work together in good faith to amend this Addendum to comply with changes in applicable law.

11. MISCELLANEOUS: This DPA supplements the Agreement. Any claims brought under this DPA will be subject to the terms and conditions of the Agreement, including the exclusions and limitations set forth in the Agreement, provided that in no event will any party be deemed to have limited its liability under the Agreement with respect to any Data Subject's data protection rights under this DPA pursuant to applicable law. This DPA shall be governed by the laws stated in the Agreement. The rights and obligations of the Parties set forth in this DPA that by their nature should survive termination or expiration of the Agreement shall survive, including, without limitation, provisions regarding confidentiality, data return or deletion, liability, audit rights, and compliance with applicable data protection laws.

APPENDIX I - DATA PROCESSING DETAILS

TYPES OF PERSONAL DATA AND OTHER REGULATED DATA PROCESSED: Company may process the following categories of data on behalf of Client:

A. Personally Identifiable Information (PII)

- Full name, alias, maiden name
- Date of birth, place of birth
- Gender, race/ethnicity (if voluntarily disclosed in HR records)
- Government-issued identifiers (SSN, driver's license, passport number)
- Email address, physical address, telephone numbers
- Citizenship and immigration status (e.g., for clearance tracking)

B. Employment and Human Resources Data

- Employee ID or system login credentials
- Job title, department, labor category
- Employment start/end dates, status, supervisor name
- Compensation details (hourly/salary, bonus, equity)
- Work schedule, timekeeping data, leave requests
- Performance evaluations, disciplinary records
- Training completion records (e.g., for cybersecurity awareness or CUI handling)
- Emergency contact information: name, relation, contact details

C. Financial and Payment Information

- Bank name and account number
- ACH routing number, SWIFT code, IBAN
- Taxpayer ID numbers
- Payroll records and withholding information
- Third Party banking details and payment instructions
- Procurement and invoice records

D. Third Party and Subcontractor Data

- Legal and trade names, business addresses
- CAGE code, DUNS number, Unique Entity Identifier (UEI)
- SAM.gov registration status
- Subcontractor POCs and contact information
- Flowdown compliance certifications and documentation

E. IT and Cybersecurity-Related Data

- IP addresses, MAC addresses, and device IDs
- System hostnames and asset identifiers
- Access logs and audit trails
- Login timestamps, session data, multi-factor authentication logs
- Email headers and metadata
- Network topology, firewall rules, endpoint telemetry
- Alerts and incident response logs
- Security event and information management (SIEM) output

F. Controlled Unclassified Information (CUI)

To the extent Client is a covered contractor or subcontractor under DFARS 252.204-7012 and related obligations, Company may access CUI as defined by:

- 32 CFR Part 2002
- NARA's CUI Registry (e.g., export-controlled data, critical infrastructure, legal privilege, proprietary business data)
- DoD program information or contract performance data marked as CUI
  This includes, but is not limited to:
  - Technical information, diagrams, or specifications
  - Contract deliverables or reports

- IT system security plans (SSPs), POAMs, or related artifacts
- FOUO and distribution-restricted documents

Note: Company will only process CUI where explicitly authorized under the Agreement and relevant Statements of Work and where Client confirms Company has a lawful basis and contractual obligation to access such data. CUI handling will comply with NIST SP 800-171 and CMMC Level 2 standards unless otherwise specified in writing.

CATEGORIES OF DATA SUBJECTS:

Company may process data relating to the following data subjects:

- Client employees, officers, directors, and interns
- Client contractors, consultants, and agents
- Client Third Partys, subcontractors, and Third Party service providers
- Client customers, representatives, and their authorized users
- Government personnel whose data is embedded in contract deliverables, reports, or communications
- Other individuals whose data is processed incidentally or indirectly in the course of delivering MSP services (e.g., data subjects referenced in helpdesk tickets or system logs)

APPENDIX II – MINIMUM TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

In accordance with applicable Data Protection Laws, DFARS 252.204-7012, NIST SP 800-171, and the Cybersecurity Maturity Model Certification (CMMC), Company shall implement and maintain the following technical and organizational measures to protect Client Data, including but not limited to Personal Data and Controlled Unclassified Information (CUI). These measures are designed to ensure a level of security appropriate to the risk and the sensitivity of the data processed.

1. Access Control

- Unique user identification for all personnel with access to systems processing Client Data.
- Role-based access control (RBAC) enforced through Active Directory or equivalent.
- Multi-factor authentication (MFA) for all administrative and remote access.
- Access logs retained, reviewed, and monitored in accordance with retention policy.
- Timely revocation of access upon employee or contractor separation or role change.

2. Data Protection

- Encryption of Client Data at rest using FIPS 140-2 validated cryptographic modules.
- Encryption of Client Data in transit using TLS 1.2 or higher.
- Logical separation of customer environments to prevent cross-tenant data access.
- Periodic data backups encrypted and stored securely, with tested restoration procedures.
- Strict controls to ensure CUI is not transmitted outside approved environments (e.g., GCC High or DoD IL4 environments if required).

3. System and Communications Security

- Secure configuration baselines applied to all systems (e.g., CIS benchmarks).
- Firewalls, intrusion detection/prevention systems (IDS/IPS), and endpoint protection.
- Network segmentation for production, staging, and management networks.
- Continuous monitoring of network traffic and system activity using SIEM tools.
- Logging of all access to CUI or Personal Data for auditing purposes.

4. Physical and Environmental Security

- Restricted physical access to data centers and workspaces containing Client Data.
- Video surveillance, entry logging, and badge-controlled access at all facilities.
- Environmental controls to protect against fire, flood, and power failure.

5. Personnel and Training

- Background checks conducted in accordance with NIST 800-171 requirements.
- Mandatory security awareness training for all employees upon hire and annually.
- Specific training for staff handling CUI, PII, and privileged systems.
- Confidentiality and acceptable use agreements signed by all personnel.

6. Third Party and Sub-Processor Management

- Sub-Processors reviewed and approved based on security and compliance posture.
- Sub-Processors handling CUI or sensitive data must meet equivalent standards.
- Flow-down of data protection obligations and CMMC/NIST alignment in contracts.
- Right to audit or receive audit documentation from Sub-Processors upon request.

7. Incident Response and Breach Notification

- Documented incident response plan aligned with NIST SP 800-61.
- 24x7 monitoring and response capabilities for detecting and containing threats.
- Notification to Client of confirmed Data Breaches without undue delay and in accordance with the terms of the Agreement and applicable laws.
- For CUI-related incidents, notification within 72 hours and reporting via DoD reporting portals as required by DFARS 252.204-7012.

8. System Security and Maintenance

- Regular vulnerability scanning and patch management.
- Endpoint Detection and Response (EDR) deployed and centrally managed.
- Annual penetration testing by qualified third parties.
- Systems hardened and updated to remove unused services, software, and ports.

9. Data Retention and Disposal

- Data retained only as long as necessary to fulfill the Services or as required by law.
- Secure deletion processes for digital media in accordance with NIST SP 800-88 Rev. 1.
- Physical destruction of retired storage devices through certified shredding or degaussing.

10. Audit and Compliance

- Maintenance of security documentation and evidence to demonstrate compliance with this Addendum and applicable laws.
- Participation in audits or assessments as agreed in the Agreement or required by law.
- Annual review and update of policies, controls, and security practices.

EXHIBIT B

ACCESS CONTROL POLICY

1. DEFINITIONS:
All capitalized terms not otherwise defined herein shall have the meanings given in the MSA.

"Change Control Board" means the internal governance body designated by Company to review, approve, and document proposed changes to client environments, administrative access, configurations, or service delivery processes. The Change Control Board operates in accordance with Company's internal Change Management policies to ensure that all changes are evaluated for security, compliance, operational impact, and alignment with contractual obligations.

"Change Management" refers to the formalized process used to evaluate, approve, document, and implement modifications to an organization's information systems, networks, or security configurations. The objective of change management is to ensure that changes, whether technical, procedural, or administrative, are introduced in a controlled and secure manner that minimizes risk and maintains the confidentiality, integrity, and availability of systems and data. In the context of CMMC, an effective change management process supports compliance with requirements related to configuration management, access control, and system integrity, and typically involves change requests, impact analysis, authorization, testing, and post-implementation review.

"RBAC" or **"Role-Based Access Control"** means the method of managing user access to systems and resources by assigning permissions based on the user's job responsibilities or role within an organization. Under this model, access rights are grouped by role name, and access to resources is restricted to only those roles that require it for the performance of specific job functions. RBAC is designed to enforce the principles of least privilege and separation of duties to enhance security and compliance**.**

"Roles" means the permission sets assigned to Security Groups to enable job-specific functions in accordance with the principle of least privilege.

"Security Groups" means the logical groupings within the Client's environment used to manage administrative access, as created and maintained by Company.

2. PURPOSE: This Exhibit outlines the administrative access and role assignment protocols that govern Company's provision of the Managed Services. This Change Management process enables secure and efficient service delivery while meeting the requirements of least privilege, segregation of duties, and applicable compliance frameworks, including NIST SP 800-171 and CMMC.

3. SCOPE OF ADMINISTRATIVE ACCESS: As Client's Managed Services provider, Company will require administrative access to the Client's Environment, including but not limited to Active Directory, Azure Active Directory, Microsoft Intune, Microsoft 365, and related systems. Company will manage administrative access using the following principles: (a) access will be provisioned via Security Groups with predefined Roles; (b) Roles will be crafted to align with job functions and security requirements; and (c) all privileged users assigned to the Client's tenant will hold certifications or possess equivalent demonstrated technical proficiency consistent with IAT Level II standards and will have undergone background screening pursuant to Company's internal personnel policies.

4. ROLE-BASED ACCESS CONTROL (RBAC) IMPLEMENTATION: Company will create Security Groups within the Client's tenant. Roles and permissions applied to these Groups may be added, modified, or removed at Company's discretion to ensure effective support and compliance. Company will assign or remove Company personnel from these Security Groups as needed. All administrative access will conform to the principle of least privilege and will be subject to internal oversight by Company's Change Control Board.

5. CHANGE MANAGEMENT PROCESS: All changes to administrative roles or assignments will be: (a) **s**ubmitted and

documented through Company's ticketing system; (b) communicated to the Client via a ticket prior to implementation; and (c) subject to internal review and approval by Company's Change Control Board. No Client action is required unless otherwise specified in the ticket. This process is intended to streamline operations while ensuring transparency and auditability.

6. INDICATORS FOR CHANGE: Administrative access changes may be initiated under the following conditions: (a) Company personnel changes, including hiring, termination, reassignment, or promotion; and (b) adjustments to improve security posture or maintain compliance with regulatory or contractual obligations.

7. OPERATIONAL AND SECURITY IMPACT: This RBAC model: (a) standardizes access by role; (b) reduces risk through segregation of duties; and (c) ensures accountability via audit trails and centralized group management.

8. TESTING AND BACKOUT PLAN:

- **Testing Plan**: Not applicable.
- **Backout Plan**: Reversal of the specific configuration change or restoration of the previous configuration state from known backups/version control.

9. ACKNOWLEDGMENT AND APPROVAL: By executing the applicable Statement of Work, Client acknowledges and approves this Change Management and RBAC protocol for the term of the Agreement.