# Commercial Terms of Service (for Federal Customers) TRINITY CYBER

## Overview of Trinity Cyber Contracting

The Terms of Service (ToS) are the contractual terms governing your subscription to Trinity Cyber services. To help explain Trinity Cyber's approach to contracting, we present a short outline immediately below. If you have any questions, be sure to visit TrinityCyber.com or contact our team.

I. Basics

The ToS are legal agreements that outline each party's rights and obligations, including (1) what you can expect from us as your service provider, (2) what we expect from you when you use the applicable product, and (3) our business practices. Unless otherwise noted, the ToS is a global document, intended to simplify contracting across regions.

II. URL Terms

Additional terms, collectively called the "URL Terms" are additional contractual terms specific to one or more products or services, found on the Trinity Cyber product or platform webpages and service terms webpage, and incorporated by reference into the ToS, covering topics such as service descriptions, support processes, Service Level Agreements (SLAs), and acceptable use policies. For the government, URL Terms are incorporated into the PWS or SOW portion of the contract.

III. Organization

The ToS are broadly organized in three general parts, collectively the Trinity Cyber **Commercial Subscription Agreement**.

i. The terms that describe the business and legal relationship between you and Trinity Cyber for your use of Trinity Cyber products, including definitions of key concepts.

ii. Region-specific terms that apply if your billing address is in the applicable region.

iii. Additional product related terms, collectively called the "URL Terms."

Trinity Cyber has made good faith attempts to remove any commercial terms that may conflict with federal law, however, should any terms herein be construed as conflicting with or be construed to require the federal government to violate an applicable statute, such term shall be considered void and the remaining terms herein shall continue with full force and effect.

## Terms of Service

These Trinity Cyber Terms of Service together with the additional terms incorporated herein by reference (the "Commercial Subscription Agreement" or "Agreement") are entered into by Trinity Cyber and the entity or person agreeing to them (including by accepting an Order or Quote that references these Terms of Service) ("Company") and govern Company's access to and use of the Services. "Trinity Cyber" has the meaning given in Section 13.11.

## 1. Services and Term

***1.1*** ***Services.*** Pursuant and subject to this Agreement, and in consideration of payment by Company of agreed upon fees under the applicable Order, Trinity Cyber will: (i) tune, maintain, update, and operate its technology as a service and provide ancillary professional services necessary to provide the security benefits of its Solution Services to Company; (ii) provide Company credentials to access Trinity Cyber's Customer Portal, and (iii) make all reasonable efforts, with Company's assistance, to move Company's Internet Traffic through Trinity Cyber's technology. Company will receive the full set of commercially released Solution capabilities and will not be charged as additional capabilities are commercially developed and added to the Solution's commercial capability.

***1.2*** ***Term.*** Unless otherwise set forth in an Order, the Initial Term for Solution subscriptions is one year. Unless otherwise set forth in an Order or Quote, at the end of the Initial Term, Solution subscriptions ordered hereunder will renew for up two successive Renewal Terms equal in length to the Initial Term unless and until terminated as provided herein. Annual escalation fees may apply.

## 2. Service Changes and Access

***2.1*** ***Service Change.*** Upon at least thirty (30) days' advance written notice to Trinity Cyber personnel, Company may request to (i) add segments of its Internet traffic, (ii) change connection options, and (iii) add extra services, which might carry additional fees. Changes to connection

options can require coordination among Trinity Cyber network engineers and Company personnel to effectuate the requested change. Careful, good faith coordination among the Parties is required to establish in advance a mutually-agreed-upon effective date and time for service changes.

***2.2 Trinity Cyber's Customer Portal.*** In leveraging the Solution on behalf of Company hereunder, Trinity Cyber shall give Company's Authorized Users access to Trinity Cyber's Customer Portal to allow Company to view the performance of the Solution. Company acknowledges that the Trinity Cyber Customer Portal was developed at private expense and therefore Trinity Cyber hereby grants Company a limited, worldwide, non-exclusive and non-transferable right and license during the Term to allow Company's designated employees and independent contractors who are authorized by Company ("***Authorized Users***") access and use of: (a) Trinity Cyber's Customer Portal through the Internet; and (b) documentation relating to the Solution, solely in and for Company's own internal purposes and business operations and in accordance with the terms and conditions of this Agreement, including, "limited" and "restricted" rights, as defined and applicable under FAR 52.227-14, Rights in Data-General, FAR 52.227-19, Commercial Computer Software License, and DFARS 252.227-7015, Technical Data – Commercial Product and Commercial Services.

***2.3 Authorized Users.*** Company (or, if requested by the Company, Trinity Cyber) will assign each Authorized User a unique account name and password to access Trinity Cyber's Customer Portal (each, a "***User ID***"). Company shall be responsible for any and all acts and omissions of its Authorized Users, and Company shall ensure that its Authorized Users abide by its data handling processes and all local, state, national, and foreign laws, and regulations, as applicable.

***2.4 User IDs and Trinity Cyber's Customer Portal.*** Company shall be responsible for ensuring the security and confidentiality of all User IDs. To the extent permitted by law, Company acknowledges and agrees that it will be fully and solely responsible for all liability incurred through the use of a User ID, and that use of Trinity Cyber's Customer Portal under any User ID will be deemed to have been performed by Company. Should Company become aware of an unauthorized use of a User ID and/or Trinity Cyber's Customer Portal ("***Unauthorized Access***"), Company shall notify Trinity Cyber immediately of the occurrence and of its efforts to remediate the effects of the Unauthorized Access and prevent a future occurrence.

***2.5 Restrictions and Company Obligations.*** Pursuant to the license terms of Section 2.2, the Company shall not permit, either directly or indirectly, any person or third party (including affiliates of Company) other than the Authorized Users to access, view, or use Trinity Cyber's Customer Portal. Company shall not, and shall ensure that its Authorized Users do not: (a) transfer, distribute, sell, lease, license, or otherwise make any aspect or portion of the Solution available to a third party; (b) reproduce, copy, translate, modify, adapt, decompile, disassemble, create Derivative Works of, reverse engineer the object code version of, or otherwise attempt to secure the source code of, all or any part of the Solution or access the Solution in order to build a similar or competitive product or service, except strictly as and to the extent expressly authorized by Applicable Laws; (c) obfuscate, remove, or alter any of the logos, trademarks, Internet links, patent or copyright notices, confidentiality or proprietary legends or other notices or markings that are on or in the Solution or documentation describing it unless performed by Trinity Cyber as contracted for herein; (d) intentionally send or store viruses, worms, time bombs, Trojan horses, or any other harmful or malicious code, files, scripts, agents, or programs; (e) intentionally interfere with or disrupt the integrity or performance of Trinity Cyber's Customer Portal, any of Trinity Cyber's other systems, infrastructure, or technology, or the data accessible through Trinity Cyber's Customer Portal; (f) attempt to gain unauthorized access to Trinity Cyber's systems or networks or any other accounts, computer systems, or networks through hacking, password mining, or other means; or (g) cause or permit reverse engineering of any Confidential Information or decompilation or disassembly of any software programs that are part of the Solution. The term "***Derivative Work***" means any derivative work of, translation, modification, adaption, enhancement, upgrade, addition, development, or improvement to an underlying intellectual property asset. At all times, Company shall comply with all Applicable Laws (as defined herein), including without limitation all federal or state data-privacy, security, or consumer-protection laws relating to the use, confidentiality, security, and privacy of data. In the course of such compliance, Company shall follow all reasonable cybersecurity practices and shall address the specific cybersecurity vulnerabilities in its networks and systems that Trinity Cyber brings to Company's attention in the course of operating the Solution. Company shall obtain any consents required for Trinity Cyber to access and use Company's systems and data for purposes of operating the Solution for Company's benefit. Company shall cooperate with Trinity Cyber as required for Trinity Cyber to properly perform its obligations, including by providing Trinity Cyber access to data and systems and supporting its discussions with Internet Service Providers or Internet Exchange Points. Trinity Cyber shall host and retain physical control over the Solution at all times. Trinity Cyber shall have no obligation to deliver or otherwise make available to Company any copies of computer programs or code, whether in object code or source code form. Trinity Cyber shall have the sole discretion to add, remove, or make changes to the functionality or capabilities of its Solution while providing performance consistent with this Agreement.

***2.6 Monitoring.*** As permitted under applicable law, Trinity Cyber shall have the right to monitor and audit Company's use of Trinity Cyber's Customer Portal without notice and by any means, including, without limitation, remote means, to verify Company's compliance with the terms of this Agreement. Company shall be responsible for ensuring that its employees and independent contractors comply with the terms of this Agreement. Pursuant to applicable law, Company shall be liable for any breach of this Agreement by its employees or independent contractors.

## 3. Ownership and Privacy

***3.1 Trinity Cyber Assets.*** Company acknowledges and admits the commercial nature of the Solution Service and therefore the validity of, and Trinity Cyber's ownership of, all trademarks, service marks, patents, copyrights, trade secrets, and other proprietary and intellectual property rights

(collectively, "***IPR***") in or related to the Solution, documentation relating to the Solution, and Trinity Cyber Proprietary Information (as defined below) (collectively, "***Trinity Cyber Assets***"). All Trinity Cyber Assets are and shall remain the exclusive property of Trinity Cyber, whether or not specifically recognized or perfected under local Applicable Laws. Company shall not take any action that jeopardizes or could jeopardize Trinity Cyber Assets. For purposes of this Agreement, "***Trinity Cyber Proprietary Information***" means Trinity Cyber's proprietary software, methodologies, tools, specifications, drawings, sketches, models, samples, records, documentation, works of authorship or creative works, ideas, knowledge, data or other materials that have been originated or developed by Trinity Cyber or on Trinity Cyber's behalf, or otherwise purchased by, or licensed to, Trinity Cyber, and used by Trinity Cyber in the course of performing any Services. Any licenses conveyed are subject to the terms herein with "limited" and "restricted" rights, as defined and applicable under FAR 52.227-14, Rights in Data-General, FAR 52.227-19, Commercial Computer Software License, and DFARS 252.227-7015, Technical Data – Commercial Product and Commercial Services.

***3.2*** ***Feedback.*** All feedback and suggestions provided by Company to Trinity Cyber relating to the Solution or any Trinity Cyber Assets, including, without limitation, any suggested features, upgrades, countermeasures, formulas, improvements, enhancements, or modifications to Trinity Cyber Assets (collectively, "***Feedback***"), is deemed to be Trinity Cyber's Confidential Information. Trinity Cyber may use such Feedback for any purpose, including, but not limited to, commercial efforts to improve and/or modify Trinity Cyber Assets, at private and commercial expense, and Trinity Cyber owns all rights, title, and interests in and to such improvements and modifications.

***3.3*** ***Acknowledgment.*** Company shall retain and own all rights, title, and interest in and to, subject to the terms herein, Company Data (defined below y) and thus Company acknowledges and agrees that Trinity Cyber shall have no liability (including damages caused by viruses and other malicious code contained in Company Data) to Company or any third party for the content, use, accuracy, or any other aspect of Company Data.

**3.3.1** ***Company Data*** means any information regarding the business or business activities of Company or its affiliates that is not available to the general public. For the avoidance of doubt, this includes, without limitation, all information the Company or its affiliates may possess that is subject to an obligation to maintain the confidentiality of same, including, without limitation, Licensee information and includes, without limitation, any Personally Identifiable Data, Sensitive Personally Identifiable Data, and/or Payment Data that may be provided or made accessible to Trinity Cyber by Company.

**3.3.2** **"Payment Data"** means: (i) with respect to a payment card, the account holder's name, account number, service code, card validation code/value, PIN or PIN block, valid to and from dates and magnetic strip data; and (ii) information relating to a payment card transaction that is identifiable with a specific account.

**3.3.3** **Personally Identifiable Data"** means any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personally Identifiable Data may relate to any individual, including, but not limited to, any employee, former employee, service provider, former service provider, customer, prospective customer, former customer, business associates (including, without limitation, Licensees), former business associates (including, without limitation, Licensees), claimant or former claimant of the rental business car sales business or claims administration business of the Company Entities or any Licensee. Personally Identifiable Data includes, without limitation, names, addresses, telephone numbers, fax numbers, e-mail addresses, date and place of birth, driver's license number, images of driver's licenses, Internet Protocol ("IP") address, passport number, credit card information, frequent flyer and other membership reward program information and affiliations with companies or associations, information about transactions with Company Entities, such as for example but not limitation, the locations, dates and times of a customer's rental pickup and return, arrival airlines and flight numbers and rental charges incurred for such transactions.

**3.3.4** **"Sensitive Personally Identifiable Data"** means: (i) an individual's Social Security number, Taxpayer Identification Number, passport number, driver's license number or other government-issued identification number; or (b) financial account number, with or without any code or password that would permit access to the account; and/or (ii) an individual's name or a unique identification number in combination with race, religion, ethnicity, medical or health information, biometric data (e.g. fingerprints, retina scans, etc.), digital signature files (i.e. digital identification key not a scanned image of a person's signature on paper), background check information or sexual orientation.

***3.4*** ***Company Data and Privacy Protection.*** During the course of providing Solution Services, Trinity Cyber may be provided access to or otherwise obtain or handle Company Data (as defined below in this Section 3.4). Trinity Cyber agrees to protect all Company Data as detailed in this Section 3.4 This subsection remains in force unless replaced by U.S. government terms of data protection that conflict with these terms.

**3.4.1** **Privacy Protection Definitions.** For purposes of this Section 3.4, the following definitions shall apply:

**3.4.1.1** **"Affiliate"** means any corporation, partnership or other entity that at any time directly or indirectly controls, is controlled by or is under common control with such first corporation partnership or entity: "control" means the possession, directly or indirectly of the power to direct or cause the direction of the management and policies of a corporation, partnership or other entity whether through the ownership of voting securities or by contract or otherwise.

**3.4.1.2 "Payment Data"** means: (i) with respect to a payment card, the account holder's name, account number, service code, card validation code/value, PIN or PIN block, valid to and from dates and magnetic strip data; and (ii) information relating to a payment card transaction that is identifiable with a specific account.

**3.4.1.3 "Data Protection Requirements"** means, collectively, all national, state and local laws or regulations relating to the protection of information that identifies or can be used to identify an individual that apply in the jurisdictions in which Company Entities do business and that apply with respect to Trinity Cyber's handling of Company Data (including, without limitation; in the United States, the Gramm-Leach-Bliley Act and California Consumer Privacy Act ("CCPA"); in the European Union, Regulation (EU) 2016/679 ("GDPR"); in the United Kingdom, the Data Protection Act 2018; in Canada, the Personal Information Protection and Electronic Documents Act ("PIPEDA"); and in Australia and New Zealand, the Australian Privacy Act 1988 and the New Zealand Privacy Act 1993) and any self-regulatory programs to which the Company Entities subscribe, including, without limitation, any Certification, relating to the protection of data that identifies or can be used to identify an individual that apply with respect to Trinity Cyber's handling of Company Data.

**3.4.1.4 "Internal Data"** means any information regarding the business or business activities of Company or Company Entities (as defined below) that is not available to the general public. For the avoidance of doubt, Internal Data includes, without limitation, all information the Company Entities may possess that is subject to an obligation to maintain the confidentiality of same, including, without limitation, Licensee information.

**3.4.1.5 "Company Data"** means Internal Data and includes, without limitation, any Personally Identifiable Data, Sensitive Personally Identifiable Data, and/or Payment Data that may be provided or made accessible to Trinity Cyber by Company.

**3.4.1.6 "Company Entities"** means, collectively, The Company and all companies in which the Company directly or indirectly owns a majority interest, commonly called "subsidiaries" of the Company.

**3.4.1.7 "Licensee"** means a member of the network of independent third parties licensed to operate businesses using the "Company" name, service mark(s) and/or business system(s).

**3.4.1.8 "PCI Standards"** means the security standards for the protection of payment card data with which the payment card companies require merchants to comply, including, but not limited to, the Payment Card Industry Data Security Standards ("PCI-DSS") currently in effect and as may be updated from time to time.

**3.4.1.9 "Personally Identifiable Data"** means any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personally Identifiable Data may relate to any individual, including, but not limited to, any employee, former employee, service provider, former service provider, customer, prospective customer, former customer, business associates (including, without limitation, Licensees), former business associates (including, without limitation, Licensees), claimant or former claimant of the rental business car sales business or claims administration business of the Company Entities or any Licensee. Personally Identifiable Data includes, without limitation, names, addresses, telephone numbers, fax numbers, e-mail addresses, date and place of birth, driver's license number, images of driver's licenses, Internet Protocol ("IP") address, passport number, credit card information, frequent flyer and other membership reward program information and affiliations with companies or associations, information about transactions with Company Entities, such as for example but not limitation, the locations, dates and times of a customer's rental pickup and return, arrival airlines and flight numbers and rental charges incurred for such transactions.

**3.4.1.10 "Sensitive Personally Identifiable Data"** means: (i) an individual's Social Security number, Taxpayer Identification Number, passport number, driver's license number or other government-issued identification number; or (b) financial account number, with or without any code or password that would permit access to the account; and/or (ii) an individual's name or a unique identification number in combination with race, religion, ethnicity, medical or health information, biometric data (e.g. fingerprints, retina scans, etc.), digital signature files (i.e. digital identification key not a scanned image of a person's signature on paper), background check information or sexual orientation.

### 3.4.2 Agreement and Compliance with Applicable Laws

**3.4.2.1** All references herein to Company Data are to data that is provided to, or obtained, used, accessed, maintained or otherwise handled by Trinity Cyber in connection with providing the Services to Company.

**3.4.2.2** Trinity Cyber will at all times comply with and treat Company Data, including Sensitive Personal Data and Payment Data, if applicable, in accordance with the requirements of this Section 3.4 and applicable Data Protection Requirements. Trinity

Cyber hereby represents and warrants that it will inform itself regarding, and comply with, all applicable Data Protection Requirements and all applicable PCI Standards. Trinity Cyber will notify Company if Trinity Cyber believes that Company's instructions concerning Sensitive Personal Data, including, without limitation, the requirements of this Section 3.4, would cause Trinity Cyber to violate any Data Protection Requirement or PCI standards.

**3.4.2.3** To the extent applicable that Trinity Cyber has access to Payment Data, Trinity Cyber shall: (a) ensure that its information security program complies with the requirements of the PCI Standards; (b) maintain a complete audit trail of all transactions and activities associated with Payment Data: and (c) not store card validation codes/values, complete magnetic strip data or PINs and PIN blocks (even if such data is encrypted). Trinity Cyber represents and warrants that it shall maintain certification of its compliance with PCI Standards and that it shall undergo independent, third-party system vulnerability scans quarterly. Trinity Cyber shall promptly provide, at the request of Company, current certification of compliance with PCI Standards by an authority recognized by the payment card industry for that purpose. If during the term of the Agreement, Trinity Cyber undergoes, or has reason to believe that it will undergo, and adverse change in its certification or compliance status with the PCI Standards and/or other material payment card industry standards, it will promptly notify Company of such circumstances. Trinity Cyber further represents and warrants that it shall not take any actions that will compromise Company's ability to comply with the PCI Standards.

**3.4.3 Data Ownership, Transfer, and Use**

**3.4.3.1** At no time shall Trinity Cyber acquire any ownership, license, rights, title or other interest in or to Company Data, all of which shall, as between Company and Trinity Cyber, be and remain the proprietary and confidential information of Company.

**3.4.3.2** In no event may Trinity Cyber: (a) use Company Data to market its services or those of an affiliate or third party; or (b) sell, rent, or otherwise monetize Company Data in any form or manner whatsoever.

**3.4.3.3** Trinity Cyber will hold Company Data in strict confidence and will not, except as may be permitted by this Agreement, disclose Company Data to any third party, firm or enterprise (including, without limitation, Trinity Cyber's affiliates) or use (directly or indirectly) any Company Data for any purpose other than in generic form to improve its security controls or as specifically directed by Company in writing and in accordance with the Data Protection Requirements. In addition, Trinity Cyber may not store or physically transfer Company Data in or to any location outside the United States without receiving the prior written consent of Company.

**3.4.3.4** Prior to providing Company Data to any third party, including, without limitation, Trinity Cyber's affiliates or a potential subcontractor or service provider, Trinity Cyber must obtain written approval for such disclosure from an officer of Company. If Trinity Cyber is permitted to disclose Company Data to such third party, such disclosure must be limited to the minimum Company Data necessary for the third party to fulfill its obligations to Trinity Cyber in support of the Trinity Cyber's Services under the Agreement. Trinity Cyber agrees that if Company consents to Trinity Cyber's disclosure of Company Data to such third party, before making such disclosure Trinity Cyber will enter into a written agreement with the third party that includes obligations that are at least as broad in scope and restrictive as those under this Section 3.4. Nonetheless, Trinity Cyber shall remain at all times accountable and responsible for all actions by such third parties with respect to the disclosed Company Data.

**3.4.3.5** Trinity Cyber represents, warrants, and covenants that it has at least one compliant transfer mechanism in place under GDPR. Trinity Cyber agrees that this Section 3.4 incorporates by reference the European Commission Implementing Decision (EU) on Standard Contractual Clauses for the Transfer of Personal Data from Controllers to Processors Established in Third Countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("Model Processor Contract"), where Trinity Cyber shall be deemed for the purposes of this Section 3.4 to be the "data importer," each of Company's affiliates established in the EU shall be deemed for the purposes of this Addendum to be the "data exporter," and the description of the transfer(s) in Annex I.B to the Model Processor Contract shall be the data processing activities in the Agreement and applicable Statements of Work which are such activities necessary for Trinity Cyber to perform its services for Company as described in this Agreement, and the data security measures in Annex II to the Model Processor Contract shall be those identified in this Agreement.

**3.4.3.6** At the request of Company, Trinity Cyber and any affiliate or subcontractor of Trinity Cyber will enter into a separate data processing agreement that incorporates the European Commission Standard Contractual Clauses between Controllers and Processors, or any similar agreement relating to other countries, with one or more of the Company Entities in order to allow Personally Identifiable Data to be transferred to Trinity Cyber and any affiliate or subcontractor of Trinity Cyber by Company Entities operating outside the United States.

**3.4.3.7** Trinity Cyber shall provide Company with a destruction schedule for Company Data and as appropriate, regularly dispose of Company Data that is maintained by Trinity Cyber, but that is no longer necessary to provide Services. Notwithstanding the foregoing, Trinity Cyber shall comply with Company's written instructions to preserve Company Data in connection with any investigations, lawsuits or other disputes in which any Company Entities may be involved. Except to perform Termination Support, upon termination or expiration of the Agreement for any reason or upon Company's request, Trinity Cyber shall immediately cease handling Company Data or any portion thereof specified by Company, and shall return in a manner and format reasonably requested by Company, or if specifically directed by Company, shall destroy any or all such Company Data in Trinity Cyber's possession, power or control, in whatever form, including without limitation all copies, fragments, excerpts, and any materials containing Company Data, whether or not such Company Data has been intermingled with Trinity Cyber's own information or materials. Upon Company's instruction to destroy or return Company Data, all copies of Company Data shall be permanently removed from Trinity Cyber's, it agents', subcontractors' and third parties' systems, records, archives and backups and all subsequent use of such Company Data by Trinity Cyber, its agents, subcontractors and third parties shall cease. Upon request, an officer of Trinity Cyber will certify to Company that all forms of the requested Company Data have been destroyed by providing certificate of destruction containing a description of the data, media type, method of disposal, date of disposal, and signature of Trinity Cyber's authorized management staff.

**3.4.4 Security and Access**

**3.4.4.1** Trinity Cyber shall develop, implement, maintain, monitor and comply with a comprehensive, written information security program that contains administrative, technical and physical safeguards to protect against anticipated threats or hazards to the security, confidentiality or integrity of, the unauthorized or accidental destruction, loss, alteration or use of, and the unauthorized access to or acquisition of Company Data. In addition, Trinity Cyber shall provide Company with documentation of such safeguards every twelve (12) months from the effective date of this Agreement and prior to any material change.

**3.4.4.2** Trinity Cyber will ensure that its information security program is consistent with: (i) Company's information security practices and requirements and which may be updated and issued to Trinity Cyber by Company from time to time; (ii) as applicable, enhanced security provisions governing the use of Sensitive Personal Data in order to comply with all applicable laws, including, without limitation, the Data Protection Requirements (including, without limitation, if applicable, the Massachusetts data security regulations (201 Mass. Code Regs. §§ 17.01 – 17.05)); (iii) as applicable, current PCI Standards; and (iii) other applicable and prevailing standard industry practices.

**3.4.4.3** Trinity Cyber will conduct a risk assessment at least annually, and more frequently if consistent with industry standards, or as may otherwise be reasonably requested by Company, to identify and assess reasonably foreseeable internal and external risks to the security, confidentiality and integrity of electronic, paper and other records containing Company Data, and evaluate and improve, where necessary, the effectiveness of its safeguards for limiting those internal and external risks.

**3.4.4.4** Trinity Cyber shall review and, as appropriate, revise its information security program: (a) at least annually or whenever there is a material change in Trinity Cyber's business practices that may reasonably affect the security or integrity of Company Data; (b) in accordance with prevailing industry practices; and/or (c) as reasonably requested by Company. If Trinity Cyber modifies its information security program following such a review, Trinity Cyber shall promptly notify Company of the modifications and shall provide the modifications to Company in writing. In the event that Trinity Cyber alters or modify its information security program in such a way that will weaken or compromise the confidentiality and security of Company Data, Company reserves the right, among other remedies under this Agreement, to terminate the Agreement without penalty or suspend Services and payment due. Such termination or suspension will not be considered Company's breach of the Agreement.

**3.4.4.5** Trinity Cyber agrees that: (a) it will establish, maintain and comply with appropriate access controls consistent with then-current industry best practices, which as of the inception of the Agreement, includes but is not limited to, limiting access to Company Data to the minimum number of Trinity Cyber employees and personnel who require such access in order to provide the Services to Company; (b) its employees and personnel who will be provided access to, or otherwise come into contact with, Company Data will be required (including during the term of their employment or retention and thereafter) to protect such Company Data in accordance with the requirements of this Section 3.4; (c) its employees and personnel who will be provided access to, or otherwise come into contact with, Company Data will have the appropriate qualifications and references (including, without limitation, a requirement that Trinity Cyber conduct background checks of such employees and personnel appropriate for the Company Data to which such employee or personnel is to be given access, prior to such employees or personnel accessing any Company Data) to handle and to protect such Company Data in accordance with the requirements of this Section 3.4; and (d) Trinity Cyber will provide such employees and personnel with appropriate training regarding information security, which shall include, to the extent applicable, the handling of Personally Identifiable Data and

Special Personally Identifiable Data, the protection of Payment Data as well as the PCI Standards, and the protection of Company Data at least annually.

**3.4.4.6** Trinity Cyber shall maintain and enforce its information security program at each location from which Trinity Cyber provides the Services. In addition: (a) Trinity Cyber shall ensure that its information security program covers all networks, systems, servers, computers, notebooks, laptops, PDAs, mobile phones, and other devices and media that process or handle Company Data or that provide access to Company Data, or the networks, systems or information of the Company Entities. Moreover, Trinity Cyber shall ensure that its information security program includes, without limitation, industry standard password protections, firewalls and anti-virus and malware protections to protect Company Data stored on computer systems. Trinity Cyber shall regularly test and monitor Trinity Cyber security procedures and systems, and shall conduct periodic reviews to ensure compliance with the requirements set forth herein. Trinity Cyber shall make the results of such reviews available to Company at Company's request; and (b) Trinity Cyber shall annually upon written request from Company: (i) provide Company with a copy of its SOC1/SOC2 Type II reports or equivalent external assessment report, which shall include an assessment report(s) for any third party supporting the Services, (ii) complete Company's standard information security questionnaire, which shall include responses to any questions regarding Trinity Cyber's controls for any part of the Services performed by a third party by or on behalf of Trinity Cyber, and (iii) make available an appropriate senior representative of Trinity Cyber's information security team to meet with Company's information security team to discuss any questions or concerns Company may have regarding Trinity Cyber's information security program; all of which shall be at no additional cost or expense to Company.

**3.4.4.7** Trinity Cyber shall encrypt all records and files containing Company Data in transit and at rest, using industry standard encryption tools, that Trinity Cyber: (a) transmits or sends wirelessly or across public networks; (b) stores on laptops or storage media; (c) where technically feasible, stores on portable devices; and (d) stores on any device that is transported outside of the physical or logical controls of Trinity Cyber. Trinity Cyber shall safeguard the security and confidentiality of all encryption keys associated with encrypted Company Data.

**3.4.4.8** If Trinity Cyber disposes of any paper, electronic or other record containing Company Data, Trinity Cyber shall do so by taking all reasonable steps (based on the sensitivity of the Company Data) to destroy the Company Data by: (a) shredding; (b) completely and permanently erasing and deleting; (c) degaussing; or (d) otherwise modifying Company Data in such records to make it unreadable, unreconstructable and indecipherable. Whenever Company Data is disposed, Trinity Cyber shall provide Company with certificate of destruction which shall include a description of the data, media type, method of disposal, date of disposal, and signature of Trinity Cyber's authorized management staff or custodian of records.

**3.4.4.9** If Trinity Cyber connects to the computing systems or networks of any Company Entities, Trinity Cyber agrees that: (a) Trinity Cyber will not access, and will not permit any other person or entity to access, the computing systems or networks of the Company Entities without Company's prior written authorization and any such actual or attempted access shall be consistent with any such authorization; (b) all Trinity Cyber connectivity to the computing systems and networks of Company Entities and all attempts at same shall be only through Company's security gateways/firewalls; and (c) Trinity Cyber will use the latest available, most comprehensive virus and malware detection/scanning program before any attempt to access any of the computing systems or networks of any Company Entities. Trinity Cyber shall inform Company in writing of the identity of any Trinity Cyber employees and personnel who have access to the systems or networks of Company Entities. Trinity Cyber may change the Trinity Cyber employees and personnel who have access to the systems or networks of Company Entities, provided Trinity Cyber gives prior written notice to Company and receives Company's written approval before any such change is effective.

**3.4.4.10** Company may perform periodic security assessments of the computing systems and networks of Company or Company Entities, which may include, without limitation, assessment of certain portions of the computing systems and networks of Trinity Cyber, third-party service providers of Trinity Cyber, or Licensees. Trinity Cyber agrees that if any such assessment reveals inadequate security by Trinity Cyber, or third-party service providers of Trinity Cyber, Company, in addition to any other remedies if may have, may suspend Trinity Cyber's access to the affected computing systems and networks of Company Entities until such inadequate security has been appropriately addressed. Such suspension will not be considered Company's breach of the Agreement.

### 3.4.5 Individual Rights

**3.4.5.1** Trinity Cyber must notify Company promptly in writing (and in any event within five (5) days of receipt) of any communication received from an individual relating to his or her request to access, modify or correct Sensitive Personal Data relating to the individual, and Trinity Cyber shall comply with all reasonable instructions of Company before responding to such communications.

**3.4.5.2** Upon receiving a request from Company to provide Company Data related to a specific individual or to delete, anonymize, redact, or otherwise sufficiently obfuscate the PID of a specific individual, Trinity Cyber will do so in accordance with applicable law within five (5) business days. If Trinity Cyber cannot or will not do so, Trinity Cyber must provide notice to Company with the reasons for such. If Trinity Cyber facilitates the request, Trinity Cyber must provide Company with a confirmation once completed.

### 3.4.6 Audits and Investigations

**3.4.6.1** If Trinity Cyber is requested or required (by oral questions, interrogatories, requests for information or documents in legal proceedings, subpoenas, civil investigative demands or similar processes) to disclose any Company Data to a third party, Trinity Cyber shall immediately notify Company of any such anticipated disclosure (except to the extent precluded by applicable law) and shall not disclose Company Data to the third party without providing Company notice at least forty-eight (48) hours following such request or demand, so that Company may, at its own expense, exercise such rights as it may have under law to prevent or limit such disclosure. Notwithstanding the foregoing, Trinity Cyber shall exercise commercially reasonable efforts to prevent and limit any such disclosure to only such Company Data as Trinity Cyber's legal counsel has determined is required to be produced and to otherwise preserve the confidentiality of Company Data, including, without limitation, by cooperating with Company to obtain an appropriate protective order or other reliable assurance that confidential treatment will be accorded to Company Data.

**3.4.6.2** Trinity Cyber shall establish and maintain complete and accurate books, notices, and accounting and administrative records necessary to document the proper handling of Company Data under this Section 3.4, including without limitation accounts of all transactions involving Company Data, and shall retain such records pursuant to applicable law. Upon reasonable notice to Trinity Cyber, Trinity Cyber shall permit Company, its auditors, designated audit representatives, and regulators, including, without limitation, data protection regulators, to audit and inspect, at Company's sole expense (except as otherwise provided in this Section), and no more often than once per year (unless otherwise required by Company's regulators): (a) the facilities of Trinity Cyber and any third-party service providers of Trinity Cyber previously approved by Company where Company Data is processed, stored or maintained by, or on behalf of, Trinity Cyber; (b) any computerized or paper systems used to share, disseminate or otherwise handle Company Data; (c) Trinity Cyber's security practices and procedures, facilities, resources, plans and procedures; and (d) all books, notices and accounting and administrative records required to be retained by Trinity Cyber hereunder. Such audit and inspection rights shall be, at a minimum, for the purpose of verifying Trinity Cyber's compliance with this Section 3.4. If any audit or inspection conducted pursuant to this Section 3.4 reveals a material technical issue, security problem, or other non-compliance with this Section 3.4, Trinity Cyber will pay Company's costs for conducting such audit and/or inspection and will propose an appropriate written response, including without limitation a plan for the remediation of the identified issue(s), within the time reasonably requested by Company. Upon Company's approval of such plan, Trinity Cyber will remedy the identified issue(s) according to the plan. Company will not be responsible for any additional costs or fees related to such remedy.

**3.4.6.3** Upon notice to Trinity Cyber, Trinity Cyber shall promptly assist and support Company in the event of an investigation by any regulator, including without limitation a data protection regulator or similar authority, if and to the extent that such investigation relates to Company Data handled by Trinity Cyber. Such assistance and support shall be at Company's sole expense, except where such investigation was required due to Trinity Cyber's acts or omissions, in which case such assistance and support shall be at Trinity Cyber's sole expense.

### 3.4.7 Trinity Cyber Side Security Incidents

**3.4.7.1** Trinity Cyber is responsible for any and all information security incidents involving Company Data while it is in the possession of Trinity Cyber. Trinity Cyber shall notify Company in writing by email promptly (and in any event within seventy-two (72) hours) whenever Trinity Cyber reasonably believes that there has been an unauthorized acquisition, destruction, modification, use or disclosure of, or unauthorized access to, Company Data while in Trinity Cyber's possession (**"Trinity Cyber Side Security Incident"**). After providing such notice, Trinity Cyber will investigate the Trinity Cyber Side Security Incident, take reasonable steps to eliminate or contain the exposures that led to such Trinity Cyber Side Security Incident, document all information collected as part of its investigation of the Trinity Cyber Side Security Incident, keep Company advised of the status of such Trinity Cyber Side Security Incident and all matters related thereto, and provide Company the opportunity to review and approve all public-facing communication prior to dispatch. Trinity Cyber further agrees to provide, at Trinity Cyber's sole cost, reasonable assistance and cooperation requested by Company and/or Company's designated representatives, in the furtherance of any correction, remediation, or investigation of any such Trinity Cyber Side Security Incident and/or the mitigation of any damage, including, without limitation, any notification that Company may determine appropriate to send to

individuals impacted or potentially impacted by the Trinity Cyber Side Security Incident, and/or the provision of any credit reporting service that Company deems appropriate to provide to such individuals. Unless required by law, Trinity Cyber shall not notify any individual or any third party other than law enforcement of any potential Trinity Cyber Side Security Incident involving Company Data without first consulting with, and obtaining the permission of, Company.

**3.4.7.2** To the extent that a Trinity Cyber Side Security Incident is caused by Trinity Cyber's breach of this Agreement or gross negligence or willful misconduct, Trinity Cyber will, at Trinity Cyber's sole cost (i) assist in providing notice relating to the Trinity Cyber Side Security Incident to impacted individuals or third parties as directed and approved by Company, (ii) prepare public-facing and regulatory responses and notifications and provide Company the opportunity to review and approve all communications prior to dispatch, (iii) handle all applicable public-facing and regulatory responses to the Trinity Cyber Side Security Incident and notifications thereof, and (iv) provide credit monitoring services to impacted individuals for a period of one year, if required by law.

**3.4.7.3** In addition, within thirty (30) days of identifying or being informed of a Trinity Cyber Side Security Incident, Trinity Cyber shall develop and execute a plan that reduces the likelihood of a recurrence of such Trinity Cyber Side Security Incident.

**3.4.7.4** Trinity Cyber agrees that, due to the unique nature of Company Data, the unauthorized disclosure or use of Company Data may cause irreparable harm to Company, the extent of which will be difficult to ascertain and for which there will be no adequate remedy at law. Accordingly, Trinity Cyber agrees that Company, in addition to any other available remedies, shall have the right to seek an immediate injunction and other equitable relief enjoining any breach or threatened breach of the provisions of this Section 3.4 without the necessity of posting any bond or other security.

***3.5 Company Identity.*** If the need arises to use Company Data to improve security or in connection with enhancing Trinity Cyber's Services and deliverables to Company and to other Trinity Cyber clients, such as identifying and describing a large cybersecurity threat across many sectors, Trinity Cyber shall anonymize any reference to Company and use other means to disguise the identity of Company in such data ("***Generic Data***"). Company hereby grants to Trinity Cyber a royalty-free, worldwide, transferable, sublicensable, irrevocable, perpetual license to use, copy, prepare derivative works of, distribute copies of, alter, and translate Generic Data.

## 4. Service Charges, Billing, and Payment

***4.1 Service Charges.*** In exchange for Trinity Cyber Services, Company shall pay Trinity Cyber, or the Authorized Reseller if applicable, the applicable fee set forth in the Order or Quote (the "***Subscription Fee***"). With the sole exceptions set forth under applicable termination provisions, Subscription Fees are non-refundable, regardless of whether or not Solution Services were actively used by Company during any time period.

***4.2 Payment and Payment Terms.*** Company shall pay Trinity Cyber all amounts owed pursuant to this Agreement within thirty (30) days of the date of the invoice for such amounts, without deduction, setoff, defense, or counterclaim for any reason. Subscriptions fees are non-refundable. Company shall provide to Trinity Cyber complete and accurate billing information including, but not limited to, Company's legal name, billing address, e-mail address, and the name and telephone number of an authorized billing contact. Company shall notify Trinity Cyber of any change in the aforementioned billing information within thirty (30) days of such change. This section shall not apply if the applicable Order is with an Authorized Reseller, in which case payment terms shall be as agreed between Company and the Authorized Reseller.

***4.3 Taxes.*** Unless otherwise stated, fees do not include any Taxes. Company is responsible for paying all Taxes associated with its purchases hereunder. If Trinity Cyber has the legal obligation to pay or collect Taxes for which Company is responsible under this Section, the appropriate amount shall be invoiced to and paid by Company, unless Company provides Trinity Cyber with a valid tax-exemption certificate authorized by the appropriate taxing authority.

***4.4 Method of Payment.*** The method of payment by Company to Trinity Cyber shall be electronic transfer to the applicable account identified by Trinity Cyber from time to time.

## 5. Indemnification and Intellectual Property Rights

***5.1 Intellectual Property Rights Indemnity.*** Per FAR 52.227-3, Patent Indemnity, and other applicable provisions, Trinity Cyber shall defend, indemnify and hold harmless Company, its officers, directors, employees and agents, from and against all claims, damages, obligations, losses, liabilities, costs and expenses (including reasonable attorney's fees) arising out of any third-party claim that a Trinity Cyber Asset infringes a United States IPR; provided, however, that (a) Company gives Trinity Cyber prompt written notice of any such claim; (b) Trinity Cyber will have the right to control and direct the defense of such claim; and (c) Company must fully cooperate with Trinity Cyber in such defense.

***5.2*** ***Intellectual Property Rights Exclusions.*** Trinity Cyber shall have no obligations under **Section 5.1** or any other liability for any claim of infringement or misappropriation resulting or alleged to result from: (a) any modification, alteration, or enhancement to the applicable Trinity Cyber Asset by any person or entity other than Trinity Cyber; (b) any use of the applicable Trinity Cyber Asset by Company in any manner for which the Solution was not designed; (c) the combination, operation, or use of the applicable Trinity Cyber Asset or any part thereof in combination with any equipment, software, data, or documentation not approved by Trinity Cyber; (d) materials, items, resources, or services provided or performed by Company (whether or not used in connection with or incorporated into the Solution); or (e) Company's continuing the allegedly infringing activity after being notified thereof or after being informed of and provided with modifications that would have avoided the alleged infringement.

***5.3*** ***Intellectual Property Rights Remedies.*** In the event an infringement or misappropriation claim as described in **Section 5.1** arises, or if Trinity Cyber reasonably believes that a claim is likely to be made, Trinity Cyber shall have the right, at its sole option, to: (a) modify the applicable portion of the Trinity Cyber Assets to become non-infringing but functionally equivalent; (b) replace the applicable portion of the Trinity Cyber Assets with material that is non-infringing but functionally equivalent; (c) obtain for Company the right to use the applicable portion of the Trinity Cyber Assets upon commercially reasonable terms; (d) remove the infringing or violative aspect of the Trinity Cyber Assets if it can be removed without material degradation of the applicable Trinity Cyber Asset; or (e) if none of (a)-(d) are commercially practicable, terminate this Agreement by providing written notice to Company and refund to Company a pro-rata portion of any prepaid Subscription Fees for the remaining paid period after the effective date of such termination. **Section 7** sets forth Company's sole and exclusive remedy and Trinity Cyber's entire liability with respect to IPR infringement or misappropriation claims, including patent or copyright-infringement claims and trade-secret misappropriation.

## 6. Warranties

***6.1*** ***Mutual Warranties.*** Each Party represents and warrants that: (a) it has full authority to enter into this Agreement; (b) it has not, nor will not, enter into any agreement with any third party that would prohibit or impair in any manner its ability to perform its obligations under this Agreement; and (c) it will perform its obligations under this Agreement in a professional manner and in compliance with applicable laws, or regulations or orders of duly authorized regulatory bodies with jurisdiction over Company or Trinity Cyber (as applicable) (collectively, "***Applicable Laws***").

***6.2*** ***Solution Warranties.*** Trinity Cyber represents and warrants that the Solution will perform substantially in compliance with the description herein and in the applicable, then-current URL Terms. Notwithstanding anything to the contrary set forth herein, in the event that the Solution fails to conform to the foregoing warranty in any material respect, Company's sole and exclusive remedy will be for Trinity Cyber, at its expense, to promptly use commercially reasonable efforts to cure or correct such failure, or, in the event such cure or correction is not commercially viable and completed in a commercially reasonable period of time, which in no event shall be less than thirty (30) calendar days, terminate the Agreement. The foregoing warranty is expressly conditioned upon: (i) Company providing Trinity Cyber with prompt written notice of any claim thereunder no later than thirty (30) days after discovering the non-conformity, which notice must identify with particularity the non-conformity; (ii) Company's full cooperation with Trinity Cyber in all reasonable respects relating thereto, including, in the case of modified software, assisting Trinity Cyber to locate and reproduce the non-conformity; (iii) Company performing its obligations under this Agreement; (iv) Company utilizing correct data and procedures; and (v) the absence of any alteration or other modification of the Solution by any person or entity other than Trinity Cyber.

***6.3*** ***Disclaimer.*** EXCEPT AS EXPRESSLY PROVIDED IN **SECTION 6.2**, TRINITY CYBER MAKES NO REPRESENTATIONS AND GIVES NO WARRANTIES, GUARANTEES, OR ASSURANCES OF ANY KIND, EITHER EXPRESS OR IMPLIED (IN LAW OR IN FACT), INCLUDING ANY WARRANTY OF MERCHANTABILITY, QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE OR USE, OR NON-INFRINGEMENT OR ANY REPRESENTATION, WARRANTY OR CONDITION FROM COURSE OF DEALING OR USAGE OF TRADE. TRINITY CYBER DOES NOT WARRANT THAT ANY SERVICES, THE TRINITY CYBER ASSETS OR ANY OTHER INFORMATION OR MATERIALS PROVIDED TO COMPANY HEREUNDER WILL SATISFY COMPANY'S REQUIREMENTS, WILL CONFORM TO ANY DESCRIPTION THEREOF, OR BE UNINTERRUPTED OR FREE OF OMISSIONS, ERRORS, OR DEFECTS. TRINITY CYBER DOES NOT ASSUME ANY LIABILITY WHATSOEVER WITH RESPECT TO ANY THIRD-PARTY PRODUCTS OR SERVICES. TRINITY CYBER DOES NOT GUARANTEE THAT ITS SERVICES WILL PREVENT ANY OR ALL CYBER ATTACKS OR DATA BREACHES, AND TRINITY CYBER SHALL NOT BE LIABLE TO INDEMNIFY OR HOLD HARMLESS THE COMPANY OR ANY THIRD PARTY FROM, AND SHALL NOT BE LIABLE FOR, ANY DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR HARM, INCLUDING BUT NOT LIMITED TO BUSINESS LOSSES, LEGAL COSTS, OR THE COST OF RESPONDING TO GOVERNMENT INVESTIGATIONS, THAT MIGHT RESULT FROM SUCCESSFUL OR PARTIALLY SUCCESSFUL ATTACKS ON COMPANY'S NETWORKS OR INTERNET TRAFFIC.

***6.4*** Trinity Cyber further disclaims all responsibility for any loss, injury, claim, liability, or damage of any kind resulting from, arising out of, or in any way related to Company's use of any equipment or software in connection with the Solution or the information accessible therefrom.

## 7. Limitation of Liability

***7.1*** ***Limitation on Types of Damages.*** IN NO EVENT SHALL TRINITY CYBER (INCLUDING ITS OFFICERS, EMPLOYEES, AND AGENTS) BE RESPONSIBLE OR LIABLE FOR ANY LOSS OF PROFIT, BUSINESS, REVENUE, USE, DATA, OPPORTUNITY, OR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, INCIDENTAL, PUNITIVE, OR OTHER DAMAGES WHATSOEVER, INCLUDING DOWNTIME COSTS, FAILURE TO REALIZE EXPECTED SAVINGS, LOSS OR UNAVAILABILITY OF OR DAMAGE TO DATA, OR SOFTWARE RESTORATION, ARISING OUT OF THE AGREEMENT OR COMPANY'S POSSESSION OR USE

OF THE SOLUTION OR ANY OTHER TRINITY CYBER ASSET, REGARDLESS OF THE THEORY OF LIABILITY, WHETHER UNDER CONTRACT, WARRANTY, STRICT LIABILITY, OR IN TORT (INCLUDING NEGLIGENCE) OR OTHERWISE, EVEN IF SUCH DAMAGE MAY HAVE BEEN FORESEEABLE OR TRINITY CYBER MAY HAVE BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

***7.2 Limitation on Amount of Damages.*** SUBJECT ALWAYS TO **SECTION 7.1**, IN NO EVENT SHALL TRINITY CYBER'S LIABILITY ARISING UNDER OR OUT OF THE AGREEMENT EXCEED, IN THE AGGREGATE, THE TOTAL FEES PAID HEREUNDER IN THE TWELVE (12) MONTH PERIOD PRIOR TO THE CAUSE OF THE CLAIM. THE LIMITATIONS SPECIFIED IN THIS SECTION SHALL SURVIVE AND APPLY EVEN IF ANY LIMITED REMEDY SPECIFIED IN THE AGREEMENT IS FOUND TO HAVE FAILED OF ITS ESSENTIAL PURPOSE. COMPANY ACKNOWLEDGES AND AGREES THAT THE LIMITATIONS OF LIABILITY AND RESTRICTIONS SET FORTH HEREIN ARE REASONABLE UNDER THE CIRCUMSTANCES.

## 8. General Provisions

***8.1 No Third-Party Beneficiaries.*** The Parties acknowledge and agree that this Agreement is entered into by and between, and for the sole benefit of, Trinity Cyber and Company, and their respective affiliates, and that there are no third-party beneficiaries of this Agreement.

***8.2 Confidentiality.*** Trinity Cyber acknowledges that the U.S. government is subject to confidentiality statutes including the Procurement Integrity Act and Trade Secrets Act, which prevent it from sharing confidential information.

***8.3 Relationship.*** The Parties shall at all times be independent contractors with respect to each other in carrying out this Agreement, and nothing herein renders them partners, joint venturers, agents, or employer and employee.

***8,4 Waiver.*** No delay or omission by either Party to exercise any right occurring upon any non-compliance or default of the other Party with respect to any of the terms of this Agreement shall impair any such right or be construed to be a waiver thereof.

***8.5 Severability.*** In the event any provision of this Agreement is determined by a court of competent jurisdiction to be invalid or unenforceable under Applicable Laws, such provision shall be amended and interpreted to accomplish the objectives of such provision to the greatest extent possible under Applicable Laws, and the remaining provisions of this Agreement shall continue in full force and effect.

***8.6 Survival.*** Notwithstanding anything to the contrary contained herein, all terms of this Agreement relating to confidentiality, proprietary rights, indemnification, disclaimers of warranty and limitations of liability, as well as those terms that by their nature survive any expiration or termination of this Agreement, shall survive.

***8.7 Insurance.*** Trinity Cyber shall maintain commercially reasonable levels of insurance related to its obligations hereunder.

***8.8 Force Majeure.*** Neither Party shall be liable for any failure or delay in the performance of its obligations, due to fire, flood, earthquake, elements of nature or acts of God, acts of war, military aggression, terrorism, riots, civil disorder, rebellions, nor other similar cause beyond the reasonable control of the Party affected (each, a "Force Majeure Event"). This subsection may be replaced or superseded by government contract terms on excusable delay.

***8.9 Headings.*** The headings of the various sections in this Agreement are for convenience of reference only and shall not affect the construction or interpretation of this Agreement or this Agreement.

***8.10 Modifications.*** The Agreement may be modified only pursuant to a writing executed by authorized representatives of both Parties. The Parties expressly disclaim the right to claim the enforceability of any oral modifications to this Agreement or any amendments based on course of dealing, waiver, reliance, estoppel, or other similar legal theory.

***8.11 Entire Agreement.*** The Agreement, including the Schedules attached hereto and incorporated herein by this reference, sets forth the entire and exclusive agreement between the Parties as to the subject matter hereof and supersedes all prior and contemporaneous understandings, negotiations and agreements, whether written or oral, between the Parties.

***8.12 Counterparts.*** The Agreement and any addendum thereto may be executed in one or more counterparts all of which taken together shall constitute one and the same instrument. An electronic signature shall be as legally effective as an original signature.

***8.13 U.S. Federal Agency Users.*** The Solution was developed solely at private expense and is a commercial off the shelf service within the meaning of the applicable Federal Acquisition Regulations and their agency supplements.

## 9. Definitions

***9.1*** ***Authorized Reseller.*** A company or person authorized by Trinity Cyber to sell Service subscriptions.

***9.2*** ***Customer Portal.*** The Customer Portal dashboard designed primarily to allow Company personnel to (i) monitor the actions taken by Trinity Cyber on its Internet Traffic, as well as additional useful and valuable information, and (ii) communicate directly with the Trinity Cyber Operations Center. The Customer Portal is Company facing and Company specific and is built on an Application Programming Interface (API) that provides a window into every action that Trinity Cyber performs on Company's traffic. The reporting delivered through the Customer Portal is a direct reflection of the threats disrupted by Trinity Cyber's Solution (or the threats that would have been disrupted during Burn-In mode). All threat and response data provided on the Customer Portal is specific to Company's traffic. Company may use this Internet facing application to report Errors and the correction thereof, and for submitting all manner of support requests. Communications with Trinity Cyber can also be telephonic (see Operations Center below).

***9.3*** ***Error.*** Error means a material deviation in the performance of the Solution from the then-current description.

***9.4*** ***Internet Traffic.*** The segment or segments of Company's Internet traffic to be run through the Solution, any information needed to transport it through Trinity Cyber technology, and the segment or segments of Company Internet traffic treated by Trinity Cyber Services.

***9.5*** ***Initial Term.*** One year unless otherwise stated in an Order.

***9.6*** ***Order.*** A written order or quote document from Trinity Cyber or its Authorized Reseller and accepted by Company identifying the specific Services to be delivered, prices, and other details, and making express reference to this Agreement.

***9.7*** ***Party or Parties.*** Trinity Cyber and/or Company.

***9.8*** ***Renewal Term.*** Subsequent one-year term for the Services after completion of the Initial Term, or as otherwise agreed to by the Parties, after completion of the Initial Term.

***9.9*** ***Service Date.*** The earlier of the date on which (a) Trinity Cyber notifies Company that the Solution is available for Company's traffic, or (b) Company first uses the Service.

***9.10*** ***Service Level Agreement (SLA).*** The then-current Service Level Agreement at TrinityCyber.com/service-terms, or for government customers the SLA terms included in the PWS or SOW.

***9.11*** ***Solution or Services.*** A technology enabled service in which Trinity Cyber tunes, maintains, updates, and operates, its proprietary technology on Company's Internet traffic, inspecting and taking direct actions on identified malicious traffic to render malicious traffic inert or ineffective and various other professional services designed to increase the Company's network security. Trinity Cyber' proprietary technology, understanding of cyber vulnerabilities, threat and adversary tradecraft for exploiting vulnerabilities, as well as the technical and engineering knowledge and know-how to build, maintain, tune, and operate its in-line services to detect malicious traffic and to perform near real time actions to render malicious traffic inert or ineffective, and to do so surreptitiously in ways that protect the Company and deceive and disrupt cyber attackers, are collectively the Solution and interchangeably Solution, Subscription Services, and Solution Services. Showing potential threats addressed or discovered, and the preventive actions taken by Trinity Cyber, to the Company's designated Information Technology (IT) or security operations personnel through a Trinity Cyber hosted portal is part of Subscription Services.

***9.12*** ***Tax or Taxes.*** All taxes arising in any jurisdiction, including without limitation all: sales, use, excise, gross receipts, value added, access, bypass, franchise, telecommunications, property (for co-location customers), consumption, or other taxes, fees, duties, charges or surcharges (however designated) which are imposed on or based on the provision, sale or receipt of the benefit of Solution Services, including such taxes imposed directly on Trinity Cyber or for which Trinity Cyber is permitted to invoice Company in connection with Trinity Cyber's performance under this Agreement. Taxes do not include Trinity Cyber's income taxes.

***9.13*** ***Term.*** Term means, collectively, the Initial Term and any Renewal Terms.

***9.14*** ***Trinity Cyber.*** For purposes of the Agreement, "Trinity Cyber" means Trinity Cyber, Inc., a Delaware corporation, having offices at 16701 Melford Blvd., Suite 300, Bowie, MD 20715.

***9.15*** ***URL Terms.*** URL Terms means the product description on the Trinity Cyber website at the time of the Agreement, or in the case of the government the terms included in the PWS or SOW.