CRITICAL START MDR SERVICES – TERMS OF SERVICE AGREEMENT

READ CAREFULLY. THE USE OF CRITICAL START MDR SERVICES IS SUBJECT TO THE FOLLOWING LEGAL TERMS AND CONDITIONS. THIS CRITICAL START TERMS OF SERVICE (THE "AGREEMENT") CONTAIN THE TERMS AND CONDITIONS THAT GOVERN YOUR ACCESS TO AND USE OF THE MDR SERVICES AND IS AN AGREEMENT BETWEEN CRITICAL START, INC. ("CRITICAL START") AND THE LEGAL ENTITY THAT WILL BE USING THE MDR SERVICES ("CUSTOMER") ON A PAID OR TRIAL USE BASIS, UNLESS THERE IS AN ACTIVE MASTER SERVICES AGREEMENT IN PLACE BETWEEN CRITICAL START AND CUSTOMER ("EXISTING AGREEMENT"), IN WHICH CASE THE EXISTING AGREEMENT WILL GOVERN CUSTOMER'S USE OF THE MDR SERVICES. THE AGREEMENT TAKES EFFECT WHEN YOU CLICK AN "I ACCEPT" OR "CONTINUE" BUTTON OR CHECK BOX PRESENTED WHEN YOU FIRST ACCESS ANY OF THE MDR SERVICES THROUGH THE CRITICAL START PLATFORM OR THE CRITICAL START MOBILE SOC APPLICATION (THE "EFFECTIVE DATE"). IF YOU ARE ENTERING INTO THIS AGREEMENT FOR AN ENTITY, SUCH AS THE COMPANY YOU WORK FOR, YOU REPRESENT TO US THAT YOU HAVE LEGAL AUTHORITY TO BIND THAT ENTITY.

This Agreement consists of the (1) Critical Start Base Terms, (2) MDR Services Terms, and (3) Critical Start Data Protection Agreement.

BASE TERMS

1. **Definitions**

"Affiliates" means, with respect to either party, any entity that directly or indirectly, through one or more intermediaries, controls, is controlled by, or is under common control with such party.
"Critical Start Platform" or "Platform" is the Cyber Operations Risk & Response technology platform from which Critical Start provides MDR Services.
"Customer Data" means (i) any data provided by Customer or Customer Affiliate(s) to the Critical Start Platform, (ii) Customer or Customer Affiliate's data accessed, ingested or used by Critical Start, or transmitted by Customer or its Affiliate(s) to the Critical Start Platform in connection with Critical Start's provision of the Services, including, but not limited to, Customer and/or its Affiliate's data included in any written or printed summaries, analyses, or reports generated in connection with the Services.
"Documentation" means the applicable written directions or policies relating to the MDR Services, which may be in paper or electronic format.
"Export Laws" means all applicable export laws and regulations of the United States and any other country where customer uses or accesses the Services.
"Indemnified Parties" shall mean, in the case of Critical Start, its Affiliates and subcontractors, and each their respective directors, officers, employees, contractors and agents and, in the case of Customer, Customer, its Affiliates, and each of their respective directors, officers, employees, contractors and agents.
"Intellectual Property" or **"IP"** means worldwide intellectual property, including but not limited to patents and patent applications, copyrights, and other rights in works of authorship, trademarks, trade secrets and other proprietary information of a party.
"MDR" means Managed Detection Response.
"MDR Reports" means the reports containing advisory data, threat data, vulnerability data, analyses, summaries, bulletins, and information made available to Customer in Critical Start's provision of its MDR Services.
"MDR Services" means managed detection and response services, provided 24x7, as described in the relevant MDR Services description provided by Critical Start, and includes applicable onboarding and implementation services.
"Professional Services" means professional services which may include, but are not limited to advisement, assessment, and implementation services.

"Security Breach" means confirmed use, accidental or unlawful destruction, loss or unauthorized disclosure of Customer Data or Customer confidential information.
"Security Event Data" means information collected by Critical Start in connection with its delivery of MDR Services to the Customer arising from and directly related to the log data, events, or alerts that Critical Start receives from the Customer's security controls that are within the scope of the MDR Services being provided to the Customer, including but not limited to, alerts from SIEM, endpoint protection (EP) platforms, endpoint detection and response (EDR), and other similar security controls.
"Services" means collectively, MDR Services and associated Professional Services.
"Service Order" means a physical, electronic, or online purchase order for MDR Services issued by Customer that references this Agreement and is accepted by Critical Start, including any attached or referenced MDR Services description.

2. **Services.** During the term of this Agreement and subject to the terms and conditions herein, Critical Start agrees to provide MDR Services and associated Professional Services purchased by Customer in accordance with the terms of this Agreement.
3. **Trial Use of Services and Beta Releases.** If Customer is entering into this Agreement for the purposes of evaluating the MDR Services, Critical Start agrees to provide Customer, at no charge, access to and use of the MDR Services, subject to the MDR Terms below for a period of thirty (30) days ("Evaluation Term"). Evaluation use of the MDR Services includes access to examples of detection, investigation, escalation, and incident support for a subset of incidents within the current, supported toolset within Customer's environment, access to and training on the use of the Platform, reports generated from the MDR Services and use of the Critical Start MobileSOC application. Critical Start may also provide Customers with access to early stage MDR Services ("Beta Releases") for evaluation. NOTWITHSTANDING ANYTHING TO THE CONTRARY HEREIN, CRITICAL START'S PROVISION OF THE MDR SERVICES ON A TRIAL BASIS OR BETA RELEASES AS DESCRIBED IN THIS SECTION 3 IS ON AN "AS-IS" AND "AS AVAILABLE" BASIS, WITHOUT ANY WARRANTY, SERVICE LEVEL COMMITMENTS OR LIABLITY OF CRITICAL START. CUSTOMER'S USE OF THE MDR SERVICES OR BETA RELEASES PURSUANT TO THIS SECTION 3 IS AT CUSTOMER'S OWN RISK. Critical Start may terminate Customer's use of the MDR Services under this Section 3 at any time for any reason or no reason in Critical Start's sole discretion, without liability.
4. **Warranties.** Customer represents and warrants that it has the necessary rights, power and authority to transmit Customer Data to Critical Start under this Agreement and that Customer has and shall continue to fulfill all obligations with respect to individuals as required to permit Critical Start to carry out the terms hereof, including with respect to all applicable laws, regulations and other constraints applicable to Customer Data. Critical Start warrants that (i) its personnel are adequately trained and competent to perform the Services, and (ii) the Services shall be performed in a professional manner in accordance with this Agreement and the relevant MDR Services description. Customer agrees to provide prompt notice of any service concerns and Critical Start will re-perform any services that fail to meet this standard. This Agreement states all remedies for warranty claims. To the extent permitted by law, the parties disclaim all other warranties. Customer understands that Critical Start's Services do not constitute any guarantee or assurance that the security of Customer's systems, networks and assets cannot be breached or are not at risk.
5. **Confidentiality.** Information exchanged under this Agreement will be treated as confidential if identified as such at disclosure or if the circumstances of disclosure would reasonably indicate such treatment. Confidential information may only be used for the purpose of fulfilling obligations or exercising rights under this Agreement, and shared with employees, agents, or contractors with a need to know such information to support that purpose. Confidential information will be protected using a reasonable degree of care to prevent unauthorized use or disclosure for 3 years from the date of receipt or (if longer) for such period as the information remains confidential. These obligations do not cover information that: i) was known or

becomes known to the receiving party without obligation of confidentiality; ii) is independently developed by the receiving party; or iii) where disclosure is required by law or a governmental agency.

6. **Customer Data.** During the term of this Agreement and the Services, Critical Start shall employ and maintain reasonable and appropriate safeguards designed to: (a) reasonably protect all Customer Data in Critical Start's possession from unauthorized use, alteration, access or disclosure; (b) subject to Section 4, detect and prevent against a Security Breach; and (c) ensure that Critical Start's employees and agents are appropriately trained to maintain the confidentiality and security of Customer Data in Critical Start's possession. Critical Start shall not be liable for any Security Breach resulting from a hack or intrusion by a third party (excluding access by any subcontractor of Critical Start) into Customer's network or systems unless the hack or intrusion was through endpoints or devices monitored by Critical Start and was caused directly by Critical Start's gross negligence or willful misconduct.
7. **Data Privacy.** Customer authorizes Critical Start to collect, use, store, transfer and otherwise process the personal data Critical Start obtains from Customer as a result of providing the Services for the purpose of complying with Critical Start's rights and obligations under this Agreement and for any additional purposes described pursuant to this Agreement. Each party expressly agrees that the Exhibit B Data Protection Agreement shall apply and govern all activities concerning the processing of personal data for the purposes of this Agreement.
8. **Proprietary Rights; Right to Use.** Except as specifically provided herein, no transfer of ownership of any intellectual property will occur under this Agreement.

   8.1 As to Customer. As between Customer and Critical Start, Customer will own all right, title and interest in and to (i) Customer Data, (ii) Customer IP, and (iii) all confidential or proprietary information of Customer or Customer Affiliates, including other Customer files, documentation and related materials, in each case obtained by Critical Start in connection with this Agreement. Customer grants Critical Start a limited, non-exclusive license to use Customer Data to perform the Services. Customer acknowledges and agrees that Customer's provision of any information contained in an MDR Report to an unaffiliated third party is at Customer's own risk and Critical Start disclaims all liability arising from such disclosure. Customer grants Critical Start a limited, non-exclusive, perpetual, worldwide, irrevocable license to use and otherwise process Security Event Data during and after the term hereof to develop, enhance and/or improve its Services provided to Customer and to Critical Start's customer base. Critical Start may compile or otherwise combine Security Event Data with similar data of other MDR Services recipients so long as said data is compiled or combined in a manner that will not in any way reveal the data as being attributable to Customer.

   8.2 As to Critical Start. As between Customer and Critical Start, Critical Start will own all right, title, and interest in and to the Products (defined below) and Services. This Agreement does not transfer or convey to Customer or any third party any right, title or interest in or to the Products and Services or any associated IP rights, but only a limited right of use as granted in and revocable in accordance with this Agreement. Critical Start will retain ownership of all copies of the Documentation. In addition, Customer agrees that Critical Start is the owner of all right, title and interest in all IP in any work, including, but not limited to, all inventions, methods, processes, and computer programs including any source code or object code, (and any enhancements and modifications made thereto) contained within the Services and/or Products (collectively, the "Works"), developed by Critical Start in connection with the performance of the Services hereunder and of general applicability across Critical Start's customer base, and Customer hereby assigns to Critical Start all right, title and interest in and to any copyrights that Customer may have in and to such Works; provided, however, that such Works shall not include Customer's confidential information, Customer Data, or other information belonging, referencing, identifying or pertaining to Customer or Customer Affiliates. Without limiting the foregoing, Critical Start will own all right, title, and interest in all IP in any MDR Reports made available to Customer. During the term of the Services, Critical Start grants to Customer a limited, non-

exclusive license to use such Works and MDR Reports solely for Customer to receive the Services and for Customer's or its Affiliate's internal security purposes only. Customer acknowledges that any license to the Critical Start Products, Services, Works and MDR Reports expires upon the expiration or termination of the relevant Service Order or this Agreement.

8.3 Feedback. If Customer elects to provide any suggestions, comments, improvements, information, ideas or other feedback regarding the MDR Services to Critical Start (collectively, "Feedback"), Customer hereby grants Critical Start a worldwide, perpetual, non-revocable, sublicensable, royalty-free right and license to use, copy, disclose, license, distribute and exploit any Feedback in any format and in any manner without any obligation, payment, or restriction based on intellectual property rights or otherwise, however, Critical Start will not identify Customer as the source of the Feedback.

9. **Term and Termination.** This Agreement will commence upon the Effective Date and will remain in effect until all Service Orders issued hereunder are terminated, unless otherwise terminated pursuant to this Section 9.

   9.1 Termination for Cause. Either party may terminate this Agreement, or any Service Order on written notice if the other party materially breaches this Agreement, or the specific terms of any Service Order, and fails to cure such breach within thirty (30) days after receipt of the notice. For an uncured breach on the part of Critical Start, Critical Start shall refund to Customer any prepaid Service fees on a pro-rata basis to the extent such Service fees are attributable to the period after the termination date. Except for termination arising under Section 9.2, termination of a specific Service Order will not affect the term of any other Service Order, provided the basis for terminating such Service Order is not also the basis for terminating any other Service Order where no breach exists. Termination of this Agreement for cause will have the effect of terminating all unfulfilled Service Orders.

   9.2 Termination for Insolvency/Bankruptcy. If either party becomes insolvent, unable to pay debts when due, files for or is subject to bankruptcy or receivership or asset assignment, the other party may terminate this Agreement and cancel any unfulfilled obligations. Any terms in the Agreement which by their nature extend beyond termination or expiration of the Agreement will remain in effect until fulfilled and will apply to both parties' respective successors and permitted assigns.

10. **Customer Cooperation.** Customer acknowledges that Critical Start's performance and delivery of the Services are contingent upon: (A) Customer providing safe and hazard-free access to its personnel, facilities, equipment, hardware, network and information required to deliver the Services, and (B) Customer's timely decision-making and provision of timely, accurate and complete information and reasonable assistance, including, granting of approvals or permissions. Customer will promptly obtain and provide to Critical Start any required licenses, approvals, or consents necessary for Critical Start's performance of the Services. Critical Start will be excused from its failure to perform its obligations under this Agreement and/or meet Service Level Agreements to the extent such failure is caused solely by Customer's delay in performing or failure to perform its responsibilities under this Agreement and/or the relevant Service Order.

11. **Limitation of Liability.** Except for either parties' respective indemnity obligations, the aggregate liability of each party under this Agreement shall not exceed the amounts paid or payable for the Services giving rise to the claim during the preceding twelve (12) month period. Neither Critical Start nor Customer will be liable for lost business, revenues or profits; business interruption or downtime costs; lost or corrupted data or software; loss of use of system(s) or network, or the recovery of such; indirect, punitive, special or consequential damages arising out of or in connection with this Agreement. This provision does not limit either party's liability for: unauthorized use of intellectual property, death or bodily injury caused by their negligence; acts of fraud; nor any liability which may not be excluded or limited by applicable law. Neither party will bring any claim based on any Service provided hereunder more than eighteen (18) months after the cause of action accrues.

12. **Indemnification**

12.1 Critical Start Indemnity. Critical Start shall defend, indemnify and hold harmless the Customer Indemnified Parties from any damages, costs and liabilities, expenses (including reasonable and actual attorney's fees) ("Damages") actually incurred or finally adjudicated as to any third-party claim or action alleging that the Products, Services or MDR Reports prepared or produced by Critical Start and delivered pursuant to this Agreement, infringe or misappropriate any third party's patent, copyright, trade secret, or other intellectual property rights enforceable in the country(ies) in which the Products, Services or any MDR Reports are performed or prepared for Customer by Critical Start ("Indemnified Claims"). If an Indemnified Claim under this Section 12.1 occurs, or if Critical Start determines that an Indemnified Claim is likely to occur, Critical Start shall, at its option: (i) obtain a right for Customer to continue using such Products, Services or MDR Reports; (ii) modify such Products, Services or MDR Reports to make them non-infringing; or (iii) replace such Products, Services or MDR Reports with a non-infringing equivalent. If Critical Start determines that (i), (ii) or (iii) above are not reasonably available, Critical Start may, at its option, terminate this Agreement and/or the affected Service Order and refund any pre-paid fees on a pro-rata basis for the allegedly infringing Products, Services or MDR Reports that have not been performed or provided. Notwithstanding the foregoing, Critical Start shall have no obligation under this Section 12.1 for any claim resulting or arising from: (a) modifications made to the Products, Services or MDR Reports that were not performed or provided by or on behalf of Critical Start; or (b) the combination, operation or use by Customer, or anyone acting on Customer's behalf, of the Products, Services or MDR Reports in connection with a third-party product or service (the combination of which causes the infringement).

12.2 Customer Indemnity. Customer shall defend, indemnify and hold harmless the Critical Start Indemnified Parties from any Damages actually incurred or finally adjudicated as to any third party claim, action or allegation (i) that the Customer Data infringes a copyright or misappropriates any trade secrets enforceable in the country(ies) where the Customer Data is accessed, provided to or received by Critical Start or was improperly provided to Critical Start in violation of any individual's rights, Customer's privacy policies or applicable laws (or regulations promulgated thereunder), (ii) asserting that lawful actions taken by Critical Start at Customer's direction in the performance of Services under this Agreement violates law or the rights of a third party, including without limitation claims or allegations related to the decryption, analysis of, collection or transfer of data to Critical Start, (iii) by Customer Affiliates (other than Signing Customer Affiliate(s)) arising from or relating to the Services, or (iv) arising from a third party's reliance on a MDR Report, any information therein or any other results or output of the Services. For the avoidance of doubt, Customer's indemnity obligations in clause (ii) of this Section 12.2 shall not affect Customer's rights or remedies under this Agreement.

12.3 Mutual General Indemnity. Each party agrees to indemnify and hold harmless the other party from any third-party claim or action (i) for personal bodily injuries, including death, or tangible property damage resulting from the indemnifying party's gross negligence or willful misconduct and (ii) relating to the indemnifying party's violation or alleged violation of Section 13.6 (Export Compliance), below.

12.4 Indemnification Procedures. The Indemnified Party will (i) promptly notify the indemnifying party in writing of any claim, suit or proceeding for which indemnity is claimed, provided that failure to so notify will not remove the indemnifying party's obligation except to the extent it is prejudiced thereby, and (ii) allow the indemnifying party to solely control the defense of any claim, suit or proceeding and all negotiations for settlement. In no event may either party enter into any third-party agreement which would in any manner whatsoever affect the rights of the other party or bind the other party in any manner to such third party, without the prior written consent of the other party.

13. General

13.1 Independent Contractor Relationship; No Publicity; Subcontracting; Assignment. The parties are independent contractors. Neither party will have any rights, power, or authority to act or create an obligation, express or implied, on behalf of another party except as specified in this Agreement. Neither party will use the other party's name (except internal use only), trademark, logos, or trade name without the prior written consent of the other party. Notwithstanding the foregoing, Critical Start may use

Customer's name in connection with general lists of customers and experience. Critical Start has the right to assign, subcontract or delegate in whole or in part this Agreement, or any rights, duties, obligations or liabilities under this Agreement, by operation of law or otherwise, provided that Critical Start shall remain responsible for the performance of Services under this Agreement. Otherwise, neither party may assign this Agreement without the permission of the other party, which shall not be unreasonably withheld or delayed; except that either party may assign this Agreement without the consent of the other party to a successor in connection with a merger, sale of all or substantially all of such party's assets, or other change of control.

13.2 Force Majeure. Neither party shall be liable to the other party for any failure to perform any of its obligations under this Agreement during any period in which such performance is delayed by circumstances beyond its reasonable control including, but not limited to, fire, flood, war, embargo, strike, riot, Internet Emergency or the intervention of any governmental authority (a "Force Majeure"). In such event, however, the delayed party must promptly provide the other party with written notice of the Force Majeure. The delayed party's time for performance will be excused for the duration of the Force Majeure, but if the Force Majeure event lasts longer than thirty (30) days, or fifteen (15) business days as to a Force Majeure delaying Customer's performance of its payment obligations, the other party may immediately terminate the applicable Service Order by giving written notice to the delayed party.

An Internet Emergency is a widespread disruption of Internet or electronic communications not caused by Critical Start, that renders the Services inaccessible or effectively unusable, for specific population(s) or location(s) and directly impact the ability of Critical Start to provide the Services and/or maintain Service Level Agreements.

13.3 Notices. Notices to either party under this Agreement must be in writing and sent by postage prepaid first-class mail or receipted courier service at the address below or to such other address (including facsimile or electronic) as specified in writing and will be effective upon receipt.

Critical Start:	**Customer:**
Critical Start, Inc.	
Attn: Legal	
6100 Tennyson Parkway, Suite 200	
Plano, TX, 75024	
legal@criticalstart.com	

This Section 13.3 shall apply for formal contract notices only and shall not limit the parties' ability to communicate via electronic mail or other methods as agreed to by the parties for routine communications.

13.4 Governing Law. All matters arising from or related to this Agreement shall be governed by the laws of the State of Delaware, without regard to principles of conflicts of law. The parties hereby consent to submit to the exclusive jurisdiction of the courts of the State of Delaware and of the United States of America located in the District of Delaware for any actions, suits, or proceedings arising from or relating to this Agreement. The parties disclaim the U.N. Convention on the International Sale of Goods.

13.5 Compliance with Laws. Each party agrees to comply with all laws and regulations applicable to such party in the course of performance of its obligations under this Agreement. In the event Critical Start engages in payment card transactions as a part of the Services provided hereunder, Critical Start shall comply with the Payment Card Industry Data Security Standards ("PCI DSS") and any amendments or restatements of the PCI DSS during the term of this Agreement.

13.6 Export Compliance. Customer will comply with all Export Laws where Customer uses any of the Services. Customer certifies that it is not on any of the relevant U.S. government lists of prohibited persons,

including the Treasury Department's List of Specially Designated Nationals and the Commerce Department's List of Denied Persons or Entity List. Customer will not export, re-export, ship, transfer or otherwise use the Services in any country subject to an embargo or other sanction by the United States, including, without limitation, Iran, Syria, Cuba, the Crimea Region of Ukraine, Sudan and North Korea. Customer will not use the Services for any purpose prohibited by the Export Laws.

13.7 Third Party Beneficiaries. The parties do not intend, nor will any Section hereof be interpreted, to create for any third-party beneficiary rights with respect to either of the parties.

13.8 Dispute Resolution. The parties will attempt to resolve any claim, or dispute or controversy (whether in contract, tort or otherwise) arising out of or relating to this Agreement or the Services hereunder (a "Dispute") through face-to-face negotiation with persons fully authorized to resolve the Dispute or through mediation utilizing a mutually agreeable mediator, rather than through litigation. The results of any negotiation or mediation may not be disclosed to any third party, except as necessary to comply with applicable law, as part of any regulatory filing (including, but not limited to, any filings made to the U.S. Securities and Exchange Commission), or to a party's attorneys, accountants or other advisors. Notwithstanding the foregoing, either party will have the right to seek from a court of competent jurisdiction a temporary restraining order, preliminary injunction or other equitable relief to preserve the status quo, prevent irreparable harm, avoid the expiration of any applicable limitations period, or preserve a superior position with respect to other creditors, although the merits of the underlying Dispute will be resolved in accordance with this paragraph. In the event the parties are unable to resolve the Dispute within thirty (30) days of notice of the Dispute to the other party, the parties shall be free to pursue all remedies available at law or equity.

13.9 Entire Agreement; Amendments; Severability; Section Headings; Survival. This Agreement, including any exhibits, attachments, applicable Service Orders are the entire agreement between Critical Start and Customer with respect to its subject matter and supersede all prior oral and written understandings, agreements, communications, and terms and conditions between the parties including, without limitation, any terms contained within a purchase order issued by Customer in connection with the Services or any separate security or privacy agreements executed by the parties. No amendment to or modification of this Agreement in whole or in part, will be valid or binding unless it is in writing and executed by authorized representatives of both parties. If any provision of this Agreement is void or unenforceable, the remainder of this Agreement will remain in full force and effect. Section headings are for reference only and shall not affect the meaning or interpretation of this Agreement. All provisions regarding indemnification, warranty, liability, and limits thereon, and confidentiality and/or protections of proprietary rights and trade secrets shall survive the termination of this Agreement.

EXHIBIT A-MDR SERVICES TERMS

These MDR Services Terms apply to all MDR Services and are in addition to the Base Terms and any service specific terms described in the relevant MDR Services description.

A.1 Definitions

"Portal" means the the Platform and/or MobileSOC portal by which Customer accesses the MDR Services.

"Products" mean collectively, Documentation, the MDR Services, Software, Protected Information, and Portal, or a combination thereof.

"Protected Information" means user IDs, tokens, passwords, digital signatures.

"Services Commencement Date" means the point in time which is the earlier of (a) Customer receiving login details for the MDR Services from Critical Start; or (b) Critical Start establishing communication with the contracted Customer device(s) and/or any Customer network equipment; or (c) Customer login to the Portal.

"Service Level Agreement" or **"SLA"** means Critical Start's commitment to MDR Service availability and delivery as described in the relevant MDR Services description and further described below.

"Software" means software that is provided or made available by Critical Start under this Agreement for Customer's use.

A.2 MDR Services and Right to Access. The MDR Services purchased by Customer shall be described in the relevant MDR Services description and will commence on the Services Commencement Date. Critical Start will provide Customer with: (i) Protected Information, (ii) access to and use of Software and the Portal, as necessary for Customer to receive the MDR Services and Documentation. Upon Customer's login to the Platform and acceptance of this Agreement, Critical Start grants to Customer a limited, nontransferable, royalty-free and nonexclusive license to access and use, and for Customer's Affiliate(s) to access and use, during the term of the MDR Services only, the Products provided to Customer, subject to the restrictions set forth below.

A.3 Use Restrictions. Customer (i) will use the Products for its internal purposes, or for the internal purposes of Customer's Affiliates purchasing MDR Services hereunder, and (ii) will not, for itself, any Affiliate of Customer or any third party: (a) sell, rent, license, assign, distribute, or transfer any of the Products, except as permitted under Section 13.1 of the Agreement; (b) decipher, decompile, disassemble, reconstruct, translate, reverse engineer, or discover any source code of the Software; (c) copy any Software or Documentation, except that Customer may make a reasonable number of copies of the Documentation for its internal use (provided Customer reproduces on such copies all proprietary notices of Critical Start or its suppliers); or (d) remove from any Software or Documentation any language or designation indicating the confidential nature thereof or the proprietary rights of Critical Start or its suppliers. In addition, Customer will not, and will not permit unaffiliated third parties to, (I) use the Products on a time-sharing, outsourcing, service bureau, hosting, application service provider or managed service provider basis; (II) alter any aspect of any Software; or (III) assign, transfer, distribute, or otherwise provide access to any of the Products to any unaffiliated third party or otherwise use any Product with or for the benefit of any unaffiliated third party.

A.4 Customer Responsibilities. Customer understands that (i) Critical Start's performance of MDR Services is dependent in part on the Customer's compliance with the requirements of this Exhibit and the relevant MDR Services description, (ii) it is responsible for timely delivery of the items and information listed in the following sections of this Exhibit, and (iii) it must perform the tasks, and provide access to Customer's employees, consultants, business processes, and/or systems as contemplated herein for Critical Start to be able to perform the MDR Services efficiently. The following Customer responsibilities are necessary to ensure Critical Start's ability to perform the Services:

- Provide reasonable assistance to Critical Start for performance under this Exhibit, including helping trouble-shoot technical issues within the Customer's environment as well as any services provided by third parties to the Customer that may affect the delivery of MDR Services.
- If applicable, provide a permanent, dedicated connection to support the execution of MDR Services. Customer is responsible for maintaining the functionality of Customer's components of this dedicated connection.

- Provide the necessary technical, license, and service information required for implementation prior to the commencement of MDR Services.
- Develop a network map detailing relevant aspects of Customer's network architecture and delivering it to the Critical Start team for their reference when troubleshooting.
- Provide Critical Start with accurate and up-to-date information including: the name, e-mail, landline, and mobile numbers for all designated authorized Customer point(s) of contact.
- Maintain current maintenance and technical support contracts with Customer's software and hardware vendors for any device affected by this Exhibit.
- Assign a Project Manager who is (i) responsible for all Customer aspects of the project, (ii) authorized to make all decisions relative to the Project, including identification and assignment of Customer resources, (iii) available to Critical Start MDR Services personnel throughout the Project, (iv) authorized to receive quarterly updates, and (v) responsible for acceptance of deliverables
- Assign a Project Sponsor who is available to Critical Start personnel through the life of the project and acts as an escalation point when conflicts cannot be resolved by the Customer Project Manager.

Customer is liable and responsible for each of the following: (i) the risk that results from non-compliance with any instruction provided by Critical Start as to the deployment, adjustment, or maintenance of any software, policy, or license; (ii) updating Critical Start as to any changes made to or needed from Services, which can include, but are not limited to, end point count, licensing requirements, and/or user accounts; and (iii) notifying Critical Start when deployed assets are invisible to or otherwise unavailable for monitoring. Customer acknowledges and agrees that the liabilities to be assumed by Customer pursuant to this section are intended to be independent of one another. Customer represents, warrants, covenants, agrees, and confirms that it will adhere to the terms of this provision and any direction given by Critical Start that would affect Services.

A.5 Project Management. Critical Start may designate a project manager to oversee the integration project and ongoing communications, manage Critical Start resources and be the Customer's primary contact with Critical Start regarding the on-boarding process, scheduled meetings, reporting and development or tuning requests. The Critical Start PMO may be contacted in the following methods:

Email	PMO@criticalstart.com
Toll Free 24/7 Support	(877) 684-2077 (Press 1 for Managed SOC)
Direct phone	(469) 609-8660

A.6 Scheduled Maintenance. Scheduled maintenance is any maintenance that is performed by Critical Start during a scheduled maintenance window (3:00AM CST – 3:30AM CST). Critical Start will provide a 48-hour notice via the Platform for any high-impact changes, excluding any unscheduled emergency maintenance that needs to be performed for stability or security of the platform.

A.7 Open Source Intelligence and Endpoint Isolation. Critical Start utilizes open source intelligence resources and will perform Services as specified below.

a. **Open Source Intelligence.** Critical Start utilizes open source intelligence resources for dynamic and static analysis of unknown binaries and unknown files to improve analysis, detection, and response to security threats that may impact customer environments. These resources include, but are not limited to, VirusTotal and Palo Alto Networks Wildfire.

b. **Isolations.** Unless Customer opts-out, Critical Start will isolate potentially compromised machines. Critical Start will manually isolate the machine using the endpoint solution and notify Customer of the isolation via the alert write-up procedure for escalation. The machines will remain in isolation until the threat has been remediated or Customer has specifically indicated that they accept the risk and request Critical Start remove the isolation. Should Customer opt to have Critical Start remove isolation from an affected machine: (i) associated SLAs shall be suspended until the discovered threat has been remedied, and (ii) Customer shall

waive all associated liability regarding the affected machine's removal from isolation. Customer hereby commits to identifying production impacting servers and assets that are not to be isolated unless Customer has given written authorization. Critical Start commits to isolating machines that are not on the authorized list only to prevent the spread of malicious code and lateral movement by suspected attackers. Critical Start will escalate all alerts that require isolation to Customer for their visibility and active feedback on the alert. Customers using endpoint detection and response and/or endpoint protection solutions are advised that the MDR Services have the ability to isolate machines on Customer's network and can use that functionality to protect Customer's network. Isolated machines will lose all connectivity to all other devices on Customer's network.

A.8 Security. Critical Start agrees to notify Customer promptly (within 48 hours), upon becoming aware of a Security Breach. Critical Start will, on an annual basis, have an audit conducted by a reputable and experienced accounting firm in accordance with the Statement on Standards for Attestation Engagements, Reporting on Controls at a Service Organization, developed by the American Institute of Certified Public Accountants and have such accounting firm issue a SOC 2 Type II Report (or substantially similar report in the event the SOC 2 Type II Report is no longer the industry standard) which will cover, at a minimum, the security policies, procedures and controls required by the Agreement (the "Audit Report"). Customer acknowledges that the Audit Report and/or any other information provided by Critical Start pertaining to Critical Start's security controls, policies, procedures, etc. are considered Confidential Information of Critical Start and shall be treated by Customer in accordance with the terms and conditions of the Agreement.

A.9 Subscription True Ups. Critical Start will initiate a true-up process at any time during the term upon determining that one of the following applies: (a) the number of endpoints monitored by Critical Start or the amount of XDR/SIEM ingest received in the Platform exceeds the Customer's MDR license subscriptions, or (b) there is a material change to Customer's environment that results in an increased usage of the MDR Services. For purposes of this Section A.9, "material increase" shall mean an increase in quantity of Customer endpoints monitored equal to the lesser of 100 endpoints or 10% of the initial endpoint count, or with respect to any XDR/SIEM deployment, an increase in the ingest rate of 10% over the amount of allocated ingest. Critical Start will initiate the true-up process by notifying Customer in writing, including the relevant details that support the true-up requirement. If it is determined there is a material increase as described above, Critical Start will take the necessary steps to increase Customer's subscription fees for MDR Services.

A.10 Service Order Term and Renewal. The subscription term of the MDR Services will automatically renew at the end of the then-current subscription term for an equivalent subscription term, unless either party provides written notice of nonrenewal at least sixty (60) days prior to the expiration of the then-current subscription term. The annual price of the MDR Services shall not increase by an amount greater than six percent (6%) of the prior year's fees for MDR Services.

A.11 Decommission or Turn-Down of Services. Upon the earlier of the termination of this Agreement or of the applicable Service Order, Customer, at Customer's expense, shall erase, destroy and cease use of all Software located on any Customer provided equipment. If the MDR Services contract is not renewed, Customer will have thirty (30) days from the date of termination or thirty (30) days from the date of contract expiration, whichever occurs first, to request a copy of Customer's archived data. Such requests may be submitted via e-mail. If Customer requests a copy of the archived data, Critical Start will transfer archived data to a customer owned AWS environment at Customer's expense. If this option is not available, Customer may request Critical Start download the archived data, at Customer's expense, (a) to a Customer designated location or (b) on encrypted media and shipped to Customer's specified location. Should the amount of Customer archived data be deemed by Critical Start to be too excessive to make available by download, Critical Start will store the data on encrypted media and ship it to Customer's specified location, at Customer's expense. If Customer does not request the archived data within the 30-day period described above, Critical Start will provide final notice to Customer prior to the end of the 30-day period before permanently destroying all archived data no longer under a valid Services contract.

A.12 Out of Scope Services. Customer understands that any cybersecurity event detected during Critical Start's MDR Service onboarding process that requires Critical Start resources outside the scope of the MDR Services described in this Exhibit shall subject to a separate cybersecurity event response retainer. Additional professional services may be required for such an engagement and if required, will be captured in a mutually agreed statement of work.

SERVICE LEVEL AGREEMENT

The service level commitments and remedies provided by Critical Start for the MDR Services and any associated Customer actions are described below.

1. Definitions

"Critical Event" refers to an Event originating from a Customer Alert, classified by the customer's security product at the highest level of criticality, typically labeled as "Critical" or "High."

"Customer Alert" is an alert transmitted from Customer's security products (endpoint and SIEM) to Critical Start's MDR Service.

An **"Event"** is created when a Customer Alert is received by the Platform.

"Median Time to Resolution" or **"MTTR"** is the median period of time to investigate Customer Alerts, measured after the last Security Alert related to the initial Customer Alert is added to the existing investigation. Measurement of MTTR includes Time to Detection, plus the total time spent for investigation and ends with escalation to the Customer or resolution of the Security Alert, if a determination is made by the SOC analyst that escalation to the Customer is not required.

"Monthly Service Fees" means the total monthly fees for the purchased MDR Service, excluding fees for any third-party product licenses and implementation services. The Monthly Service Fee shall be determined by taking the prepaid annual fee for the MDR Services, less the amounts for any third-party product licenses and implementation services and dividing that total by 12.

"Production Monitoring" means the point in time at which Critical Start has completed onboarding of a Customer asset to be monitored and has commenced monitoring of such Customer asset. Customer assets in Production Monitoring will be identified in the Platform dashboard and MobileSOC app.

"Security Alert" is generated when an Event is determined by the Trusted Behavior Registry to be of unknown behavior. A Security Alert may result in: (i) investigation by the Critical Start SOC, (ii) resolution by the Critical Start SOC, or (iii) escalation to the Customer for investigation. Multiple correlated Events may be aggregated into a single Security Alert. Detections within the Platform that are in active development or tuning may not generate Security Alerts..

"Time to Detection" or **"TTD"** means the period of time calculated from the point an Event is converted to a Security Alert, as shown in the Platform audit log, and ends when one of the following occur: 1) the Security Alert is assigned to an analyst, 2) the tag, priority, or a comment on Security Alert is changed, 3) the Security Alert category is changed to one that is marked Stop TTR/TTD.

"Time to Resolution" or **"TTR"** is the amount of time measured from the point in time a Security Alert is assigned to a Critical Start SOC analyst and ends when the analyst (i) responds to the Security Alert, (ii) resolves the Security Alert, or (iii) escalates the Security Alert to the Customer for investigation. TTR includes the time measured under TTD.

"Trusted Behavior Registry" is Critical Start's registry of known good behaviors.

2. Service Level Compliance. Critical Start's tracking of Service Level compliance starts after the point in time where the implementation and deployment process has been completed and Customer assets are in Production Monitoring. Customer will be notified (in writing or email) that MDR Services have transitioned from deployment phase to Production Monitoring. Service Levels will not apply and remedies will not be available during beta, evaluation, proof of concept, or testing of the MDR Service.

Customer is responsible for responding to Security Alerts escalated to Customer by Critical Start's SOC within three (3) working days from receipt of the escalation or communication. Critical Start relies on Customer's prompt response to escalated Security Alerts for resolution of open Customer Alerts and to improve the Platform performance by eliminating future false positives. TTD and MTTR SLA compliance will not be tracked during periods of time when the Customer is not responding/has not responded to multiple requests to resolve Security Alerts.

Critical Start reserves the right to modify the SLA(s) set out below from time to time, in its reasonable discretion, by providing advanced notice to Customer. Any such amendments (a) will have no material adverse impact on the MDR Services, Service Levels or Service Level credits currently being provided to Customer by Critical Start; and (b) are being effected with respect to all similarly situated Critical Start customers.

3. Exclusions from SLAs. The impact of any of the following items shall be excluded from the calculation of service level achievement.

- Traffic/events that do not reach the Critical Start SOC due to (i) the fault or delay of Customer, (ii) a failure of the network environment, internet connectivity or traffic that does not generate a logged event.
- Service interruptions, deficiencies, degradations, or delays due to (i) Customer supplied Internet or private access; (ii) power, equipment, systems or services not supplied by Critical Start, (iii) equipment, configuration, routing event, or technology required for delivery of MDR Services that is under the management or control of Customer, (iv) Customer changes to the system specifications, (v) removal of a service component by Customer without a mutually agreed to change order or (vi) the acts or omissions of third parties engaged by Customer.
- Performance of scheduled or emergency maintenance.
- Customer's noncompliance with any instruction provided by Critical Start as to (i) the deployment, adjustment, or maintenance of any software, policy, or license; (ii) recommended configurations on managed or unmanaged equipment that impacts the provision of MDR Services.
- Customer's failure to provide a suitable and secure environment for on-premise devices.
- Network, software, or server changes or outages to the managed services environment without reasonable prior notification that significantly impact event volumes. This applies to any assets that may affect the generation of and/or transmission capability of logs, and events or other activity which is monitored by Critical Start for security alerts.
- Any time period during which Customer or Customer engaged third-party initiated testing of the MDR Services is taking place.

4. Service Level Agreement

SLA CATEGORY	DESCRIPTION	SLA
Platform/MobileSOC Availability	Availability of Platform/MobileSOC application to Customer. Availability is measured by the total number of minutes in the month minus the number of minutes the Platform/MobileSOC is unavailable during the month (adjusted for any scheduled downtime) divided by the total number of minutes in the month x 100.	99.9%

Individual Security Alert Investigation – Time to Detection ("TTD")	The TTD timeframe in minutes is automatically calculated by the Platform and annotated in the Platform audit log.	60 minutes SLA metrics are available in the Platform and via the MOBILESOC app. SLA performance is measured each Monday-Sunday (UTC) period during Production Monitoring.
Monthly Median Security Alert Resolution Time SLA ("MTTR")	For a monthly basis, MTTR will be calculated as shown in the Platform or in the MOBILESOC app.	60 minutes MTTR available in the Platform and the MOBILESOC app
Time to Notification ("TTN")	If configured, Customer will be notified in the Platform for the following scenarios: • a new Security Alert is created from one or more Critical Events. • an existing Security Alert receives a correlated Critical Event, and a notification has not been previously sent for that Security Alert • a Security Alert is reclassified as "Critical" by the Critical Start SOC	10 minutes

5. Service Level Credits. Customer will receive credit for Critical Start's failure to meet the Service Level outlined above within thirty (30) days of notification by Customer to Critical Start of such failure.

Service Level credits will be calculated using the Monthly Service Fees. If it is determined that Critical Start has missed any of the above SLA categories multiple times during any single 24-hour period, Critical Start will provide and Customer's remedy is limited to a Service Level credit equal to one day of the MDR Services fee for the affected MDR Service.

CRITICAL START PLATFORM/MOBILESOC PORTAL AVAILABILITY AND NOTIFICATION SYSTEMS SLA: 99.9%

SYSTEM AVAILABILITY	CREDITS DUE CUSTOMER
99.8% - 99.9%	No Credit Due
99.5% - 99.79%	1% of the Monthly MDR Service Fee
99.0% - 99.49%	3% of the Monthly MDR Service Fee
98.5% - 98.99%	5% of the Monthly MDR Service Fee
Less than 98.5%	10% of the Monthly MDR Service Fee

INDIVIDUAL SECURITY ALERT INVESTIGATION SLA (TTD): 60 MINUTES

QTY OF SECURITY ALERTS NOT MEETING TTD SLA	CREDITS DUE CUSTOMER
10 or less	No Credit Due
11 - 20 Security Alerts	5% of the Monthly MDR Service Fee
21 or More Security Alerts	10% of the Monthly MDR Service Fee

MONTHLY MEDIAN ALERT RESOLUTION TIME SLA (MTTR): 60 MINUTES

MTTR	CREDITS DUE CUSTOMER
MTTR > SLA for Calendar Month	15% of the Monthly MDR Service Fee

TIME TO NOTIFICATION SLA (TTN): 10 MINUTES

TTN	CREDITS DUE CUSTOMER
TTN > SLA for Calendar Month	15% of the Monthly MDR Service Fee

6. Service Level Credit Payment. Customer notification of the Service Level failure must be submitted to Critical Start within thirty (30) days of the Service Level failure in order for Customer to be eligible for any Service Level credit. Critical Start will research the alleged Service Level failure and respond to Customer within thirty (30) days from the date of the request. The total amount credited to a Customer in connection with Critical Start's failure to meet any of the above Service Levels in any calendar month will not exceed fifty percent (50%) of the monthly MDR Service fees paid by Customer for the affected MDR Service.

Any Service Level credits determined to be applicable to Customer shall be accrued by Critical Start against Customer's account and made available for Customer to apply against the next annual invoice. If Customer elects to leave the MDR Service and has Service Level credits accrued to their account, Critical Start will remit the amount of the accrued Service Level Credits to Customer within 60 days of termination of the applicable Service Order or the Agreement. Payment of Service Level credits shall be Customer's sole and exclusive remedy and Critical Start's entire liability for its failure to meet the Service Level commitments set out in this Service Level Agreement.

EXHIBIT B

CRITICAL START DATA PROTECTION AGREEMENT

This Data Protection Agreement ("DPA") forms part of the Agreement between the Customer and Critical Start, Inc. ("Critical Start") and shall apply where the provision of Services by Critical Start to Customer involves the processing of Personal Data (as defined below) and is subject to Privacy Laws. Except as otherwise expressly stated, Customer is the controller and Critical Start is the processor (as defined below) of the Personal Data processed under this Agreement. Capitalized terms shall have the meaning set forth in the Agreement, unless otherwise defined in this DPA. In the event of a conflict between this DPA and the Agreement, this DPA shall control with respect to its subject matter.

1. Definitions

References in this DPA to "controller," "data subject," "processor," and "supervisory authority" shall have the meanings ascribed to them under Privacy Laws. Capitalized terms that are not defined in this DPA shall have the meaning set out in the Agreement. In this DPA:

1.1. "Data Breach" means an actual breach by Critical Start of the security obligations under this DPA leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, the Personal Data transmitted, stored, or otherwise processed.

1.2. "Personal Data" means any information relating to an identified or identifiable natural person that is processed by Critical Start, acting as a processor on behalf of the Customer, in connection with the provision of the Services, and is subject to Privacy Laws.

1.3. "Privacy Laws" means any United States and/or European Union data protection and/or privacy-related laws, statutes, directives, or regulations (and any amendments or successors thereto) to which a party of the Agreement is subject and are applicable to the Services including, without limitation, the General Data Protection Regulation 2016/679.

1.4. "Processing" (and its derivatives) means any operation(s) performed on Personal Data, whether or not by automated means, including the collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment, combination, restriction, erasure, or destruction.

1.5. "Security Event Data" means information related to security events that is collected during Critical Start's provision of Services.

1.6. "Services" means the managed security services and/or professional services provided by Critical Start to Customer.

1.7. "Sub-processor" means a third party engaged by Critical Start (including, without limitation, an Affiliate and/or subcontractor of Critical Start) in connection with the processing of the Personal Data.

2. Description of Processing. A description of the processing activities to be undertaken as part of the Agreement and this DPA are set out in Annex 1.

3. Compliance with Laws. The parties agree to comply with their respective obligations under Privacy Laws. In particular, Customer warrants and represents (on its behalf and on behalf of each of its Affiliates, where applicable) that it has obtained all necessary authorizations and consents required for compliance with Privacy Laws prior to disclosing, transferring, or otherwise making available any Personal Data to Critical Start and that it has provided appropriate notifications to data subjects describing the purpose for which their personal data will be used pursuant to this DPA and the Agreement.

4. Critical Start Obligations

4.1. Instructions. Critical Start shall process the Personal Data only in accordance with Customer's reasonable and lawful instructions (unless otherwise required to do so by applicable law). Customer hereby instructs Critical Start to process Personal Data to provide Services and comply with Critical Start's rights and obligations under

the Agreement and this DPA. The Agreement and DPA comprise Customer's complete instructions to Critical Start regarding the processing of Personal Data. Any additional or alternate instructions must be agreed upon between the parties in writing, including the costs (if any) associated with complying with such instructions. Critical Start is not responsible for determining if Customer's instructions are compliant with applicable law. However, if Critical Start is of the opinion that a Customer's instruction infringes applicable Privacy Laws, Critical Start shall notify Customer as soon as reasonably practicable and shall not be required to comply with said infringing instruction.

4.2. Confidentiality. To the extent the Personal Data is confidential (pursuant to applicable law), Critical Start shall maintain the confidentiality of the Personal Data in accordance with the confidentiality obligations of the Agreement and shall require persons authorized to process the Personal Data (including its Sub-processors) to have committed to materially similar obligations of confidentiality.

4.3. Disclosures. Critical Start may only disclose Personal Data to third parties (including, without limitation, its Affiliates and Sub-processors) for the purpose of: **(a)** complying with Customer's reasonable and lawful instructions; **(b)** as required in connection with the Services and as permitted by the Agreement and/or this DPA; and/or **(c)** as required to comply with Privacy Laws, or an order of any court, tribunal, regulator, or government agency with competent jurisdiction to which Critical Start, its Affiliates, and/or Sub-processors is subject, PROVIDED THAT Critical Start will (to the extent permitted by law) inform the Customer in advance of any disclosure of Personal Data and will reasonably cooperate with Customer to limit the scope of such disclosure to what is legally required.

4.4. Assisting with Data Subject Rights. Critical Start shall, as required in connection with Services and to the extent reasonably practicable, assist Customer in responding to requests from data subjects exercising their rights under Privacy Laws (including, without limitation, the right of access, rectification, and/or erasure) in respect of Personal Data. Critical Start reserves the right to charge Customer for such assistance if the cost of assisting exceeds a nominal amount. Critical Start shall notify Customer as soon as practicable of any request Critical Start receives from data subjects relating to the exercise of their rights under applicable Privacy Laws during the Term of the Agreement (to the extent such request relates to Personal Data).

4.5. Security. Taking into account industry standards, the costs of implementation, the nature, scope, context, and purposes of the processing and any other relevant circumstances relating to the processing of Personal Data, Critical Start shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk in respect of any Personal Data in accordance with Critical Start policies.

4.6. Sub-processors. Customer agrees that Critical Start may appoint and use Sub-processors (a list of which shall be provided upon request) to process Personal Data in connection with Services PROVIDED THAT: **(a)** Sub-processor has obligations that are (i) relevant to the Services provided by Critical Start and (ii) has implemented appropriate technical and organizational measures that are materially similar to the rights and/or obligations granted to or imposed upon Critical Start under this DPA; and **(b)** where a Sub-processor fails to fulfill its data protection obligations as specified above, Critical Start shall be liable to the Customer for the performance of the Sub-processor's obligations.

4.7. Deletion of Personal Data. Upon termination of Services (for any reason), and if requested by Customer in writing, Critical Start shall as soon as reasonably practicable delete Customer's Personal Data, PROVIDED that Critical Start may:

(a) retain one copy of Personal Data as necessary to comply with any legal, regulatory, judicial, audit, or internal compliance requirements; and/or **(b)** defer the deletion of Personal Data to the extent, and for the duration, that any Personal Data or copies thereof cannot reasonably and practically be expunged from Critical Start's systems. For such retention or deferral periods as referred to in sub-paragraphs (a) or (b) of this clause, the provisions of this DPA shall continue to apply to such Personal Data. Critical Start reserves the right to charge Customer for any reasonable costs and expenses incurred by Critical Start in deleting Personal Data pursuant to this clause.

4.8. Demonstrating Compliance. Critical Start shall, upon reasonable, prior written request from Customer (such request not to be made more frequently than once in any twelve (12) month period), provide to Customer

such information as may be reasonably necessary to demonstrate Critical Start's compliance with its obligations under this DPA.

4.9. Audit and Inspections. Where Customer reasonably considers the information provided under clause 4.8 above to not be sufficient to demonstrate Critical Start's compliance with this DPA, Customer may request reasonable access to Critical Start's relevant processing activities in order to audit and/or inspect Critical Start's compliance with this DPA PROVIDED THAT: **(a)** Customer gives Critical Start reasonable, prior written notice of at least thirty (30) days before any audit or inspection (unless a shorter notice period is required by Privacy Laws, an order of a supervisory authority, otherwise agreed between the parties, or in the event of a Data Breach); **(b)** audits or inspections may not be carried out more frequently than once in any twelve (12) month period (unless required more frequently by Privacy Laws, an order of a supervisory authority, otherwise agreed between the parties, or in the event of a Data Breach); **(c)** Customer submits to Critical Start a detailed audit plan at least two (2) weeks in advance of the proposed audit date describing the proposed scope, duration, and start date of the audit. Critical Start shall review the audit plan and provide Customer with any material concerns or questions without undue delay. The parties will then reasonably cooperate to agree a final audit plan; **(d)** Critical Start may restrict access to information in order to avoid compromising a continuing investigation, violating law, or violating confidentiality obligations to third parties. Any access to sensitive or restricted facilities by Customer is strictly prohibited due to regulatory restrictions on access to other customers' data, although Customer and/or its auditor shall been titled to observe the security operations center via a viewing window. Customer shall not (and must ensure that its auditor shall not) allow any sensitive documents and/or details regarding Critical Start's policies, controls, and/or procedures to leave Critical Start's location where the audit or inspection is taking place (whether in electronic or physical form); **(e)** Customer carries out the audit or inspection during normal business hours and without creating a business interruption to Critical Start; **(f)** the audit or inspection is carried out in compliance with Critical Start's relevant on-site policies and procedures;
(g) where the audit is carried out by a third party on behalf of the Customer, such third party is bound by similar obligations to those set out in Section 8 of the Agreement (Confidentiality) and is not a direct competitor of Critical Start. Critical Start reserves the right to require any such third party to execute a confidentiality agreement directly with Critical Start prior to the commencement of an audit or inspection; and **(h)** except where the audit or inspection discloses a failure on the part of Critical Start to comply with its material obligations under this DPA, Customer shall pay all reasonable costs and expenses (including, without limitation, any charges for the time engaged by Critical Start, its personnel, and professional advisers) incurred by Critical Start in complying with this clause.

Customer shall provide to Critical Start a copy of any audit reports generated in connection with an audit carried out under this clause, unless prohibited by applicable law. Customer may use the audit reports only for the purposes of meeting its regulatory audit requirements and/or confirming compliance with the requirements of this DPA. The audit reports shall be Confidential Information of the parties.

5. International Transfers. Critical Start may, in connection with the provision of Services, or in the normal course of business, make international transfers of Personal Data to its Affiliates and/or Sub-processors. When making such transfers, Critical Start shall ensure appropriate protection is in place to safeguard the Personal Data transferred under or in connection with the Agreement and this DPA. Where the provision of Services involves the transfer of Personal Data from countries within the European Economic Area ("EEA") to countries outside the EEA (that are not subject to an adequacy decision under Directive 95/46/EC or GDPR), such transfer shall be subject to the following requirements: **(a)** Critical Start has implemented appropriate security measures to adequately protect the transfer of Personal Data; **(b)** Critical Start has in place intra-group agreements with any Affiliates who may have access to Personal Data, bound by agreements that incorporate the EU Commission approved Standard Contractual Clauses ("Standard Contractual Clauses"); and **(c)** Critical Start has in place agreements with its Sub-processors that incorporate the Standard Contractual Clauses (as appropriate).

6. Data Breaches. Where a Data Breach is caused by Critical Start's failure to comply with its obligations under this DPA, Critical Start shall: **(a)** notify Customer without undue delay after establishing the occurrence of the Data Breach and shall, to the extent such information is known or available to Critical Start at the time, provide Customer with details of the Data Breach, a point of contact, and the measures taken or to be taken to address the Data Breach; **(b)** reasonably cooperate and assist Customer with any investigation into, and/or remediation of, the Data Breach (including, without limitation, and where required by Privacy Laws, the provision of notices to regulators and affected individuals); **(c)** not inform any third party of any Data Breach relating to Customer's Personal Data without first obtaining Customer's prior written consent, except as otherwise required by applicable law provided that nothing in this clause shall prevent Critical Start from notifying other customers whose personal data may be affected by the Data Breach; and **(d)** in the event Customer intends to issue a notification regarding the Data Breach to a supervisory authority, other regulator, or law enforcement agency, Customer shall (unless prohibited by law) allow Critical Start to review the notification and Customer shall have due regard to any reasonable comments or amendments proposed by Critical Start.

7. Liability and Costs. Neither Critical Start nor any Sub-processor shall be liable for any claim brought by Customer or any third party arising from any action or omission by Critical Start and/or Sub-processors to the extent that such action or omission resulted from compliance with Customer's instructions.

8. Security Event Data. Critical Start will process Security Event Data as part of its provision of Services. Customer acknowledges that Critical Start may also process Security Event Data in order to develop, enhance, and/or improve its security services and the products and services it offers and provides to customers. Critical Start shall be the processor in respect to any Personal Data in the Security Event Data and, for the duration of its processing of such Security Event Data, Critical Start shall: (i) comply with applicable Privacy Laws and (ii) safeguard such Security Event Data with security measures that are no less protective than those set out in this DPA. Restrictions on the disclosure and transfer of Personal Data in this DPA shall not apply in connection with Critical Start's processing of the Security Event Data for the purposes described in this clause. However, Critical Start's shall not disclose any Security Event Data that is traceable to Customer to any third parties (other than Affiliates and Sub-processors) unless permitted under the Agreement and/or this DPA, or the disclosure is required in order to comply with applicable law or legal process. Critical Start shall not be required to return or delete Security Event Data upon termination of Services (for any reason). Customer shall ensure that its personnel and any other data subjects whose Personal Data is processed by Critical Start in connection with Services are appropriately notified of the fact that their Personal Data may be processed in connection with the development, enhancement, and/or provision of Critical Start's products or services as described in this clause. If Customer is compelled by a legally-binding order (e.g. of a court or regulatory authority of competent jurisdiction) to have the Security Event Data deleted, then Critical Start agrees, as appropriate, to anonymize, pseudonymize, or delete the Security Event Data that is the subject of the binding order as soon as practicable.

9. Privacy Impact Assessments. Critical Start shall provide reasonable cooperation and assistance to Customer, to the extent applicable in relation to Critical Start's processing of the Personal Data and within the scope of the agreed Services, in connection with any data protection impact assessment(s) that the Customer may carry out in relation to the processing of Personal Data to be undertaken by Critical Start, including any required prior consultation(s) with supervisory authorities. Critical Start reserves the right to charge Customer a reasonable fee for the provision of such cooperation and assistance.

ANNEX 1 - PROCESSING DESCRIPTION

Subject Matter and Purpose

Subject to the terms of the Agreement, Critical Start provides information security services for the Customer and processes Personal Data for the purpose of providing such services as set out in applicable Service Orders, SOWs, SLAs, service descriptions, or otherwise.

Duration of Processing

Critical Start will retain and process Customer's Personal Data for the term of the Agreement and in accordance with the provisions of this DPA regarding the return or deletion of Personal Data.

Data Subjects

The Personal Data transferred may concern the following categories of data subjects: individuals who use and access Customer information technology systems for which CRITICALSTART provides services.

Type of Personal Data

- For MDR Services: Personal Data may be contained:
    - within security logs or alerts, which may include information related to IT resources access, such as username, identification number, location, IP address, MAC address, or other device identifier, resource accessed, time of access, and device name;
    - within context related to the security logs or alert that may include malicious files, network fragment, process details, domain name, network connections; or
    - within the user account created to access Critical Start MDR resources (e.g. Portal access).

- For Critical Start Consulting Services: Personal Data that maybe processed by Critical Start, if necessary, for the provision of the Consulting Services may include any or all of the following:
    - contact details, which may include name, address, e-mail address, phone and fax contact details, and associated local time zone information;
    - employment details, which may include company name, job title, grade, demographic, and location data;
    - IT systems information, which may include user ID and password, computer name, domain name, IP address, and software usage pattern tracking information i.e. cookies;
    - data subject's e-mail content and transmission data which is available on an incidental basis for the provision of information technology consultancy, support and services (incidental access may include accessing the content of e-mail communications and data relating to the sending, routing and delivery of e-mails);
    - details of goods or services provided to or for the benefit of data subjects; and
    - financial details (e.g. credit, payment and bank details)special categories of data (if appropriate) which may involve the incidental processing of personal data which may reveal: racial or ethnic origin; political opinions; religious or philosophical beliefs; trade-union membership; genetic data and bio metric data for the purpose of uniquely identifying a natural person; data concerning health (including physical or mental health or condition); sexual life or sexual orientation; criminal offences or alleged offences and any related court proceedings; social security files.