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 CRITICALSTART 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 CRITICALSTART 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 CRITICALSTART, 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 CRITICALSTART's provision of Services.

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

1.7. "Sub-processor" means a third party engaged by CRITICALSTART (including, without limitation, an Affiliate and/or subcontractor of CRITICALSTART) 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 CRITICALSTART 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. CRITICALSTART 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 CRITICALSTART to process Personal Data to provide Services and comply with CRITICALSTART's rights and obligations under the Agreement and this DPA. The Agreement and DPA comprise Customer's complete instructions to CRITICALSTART 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. CRITICALSTART is not responsible for determining if Customer's instructions are compliant with applicable law. However, if CRITICALSTART is of the opinion that a Customer's instruction infringes applicable Privacy Laws, CRITICALSTART 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), CRITICALSTART shall maintain the confidentiality of the Personal Data in accordance with Section 11 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. CRITICALSTART 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 (who are identified on the subcontractor list posted on our website, as updated from time to time) 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 the 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 controller 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.