DARKTRACE

ADDENDUM TO THE MASTER SERVICES AGREEMENT: PRODUCT SPECIFIC TERMS

Save as otherwise defined herein, any definitions referenced in this Appendix 4 shall have the meanings ascribed to them in the Agreement located at https://darktrace.com/legal/master-services-agreement.

SCHEDULE 1: Darktrace / Attack Surface Management

This Schedule (the "**Attack Surface Management Schedule**") is applicable where Customer has purchased the **Darktrace / Attack Surface Management** product offering (the "**Attack Surface Management Offering**").

1. ACCESS TO AND USE OF THE OFFERING

1.1. Customer's use of the Attack Surface Management Offering, and Darktrace's delivery of the Attack Surface Management Offering, is provided subject to the terms of the Agreement.

2. DELIVERY OF THE OFFERING

2.1. Customer hereby grants to Darktrace a non-exclusive, irrevocable (for the Subscription Period), royalty-free right to use the Search Terms (as set out in clause 3.1 below).

2.2. Where Darktrace is required to create a non-personal system account (an "**NPSA**") for Customer, Customer acknowledges and agrees that Customer shall be solely responsible for access to and activity occurring under the NPSA. Under no circumstances shall Darktrace be liable to Customer for the use of the NPSA by Customer or any third parties, or for any reports, accounts, third party or customer portals or account information connected to or generated by the NPSA.

2.3. Darktrace may provide Customer with risk assessments or reports on third parties ("**Assessments**") where Customer has a contractual right or a demonstrable, legitimate interest to request such Assessments. Where Darktrace carries out such Assessments, Customer acknowledges and agrees that Darktrace may use third party and publicly available sources to generate these Assessments

3. WARRANTIES

3.1. Customer warrants and represents that it owns or has obtained all relevant third party licenses and consents to use and provide to Darktrace any: (a) brand names; (b) keywords; (c) product names; (d) company names; and (e) any other search terms in which intellectual property rights may vest in Customer and/or a third party, each independently a "**Search Term**" and one or more together the "**Search Terms**".

3.2. Darktrace provides no warranties or representations as to the accuracy or reliability of the data generated by the Attack Surface Management Offering and any conclusions, decisions, actions or interpretations of the data provided by the Attack Surface Management Offering are inferred or taken at Customer's own risk. To the fullest extent permissible by applicable law, Darktrace accepts no liability for any actions taken or inferences made by Customer pursuant to the provisions of this clause 3.2.

4. DATA PROTECTION

4.1. In the provision of the Attack Surface Management Offering, Customer may provide to Darktrace Personal Data for which Darktrace shall be deemed a Data Controller and, in respect of such Personal Data, Darktrace shall comply fully with its obligations as a Data Controller under the Data Protection Laws.

4.2. Notwithstanding clause 4.1 above, in the event that Darktrace is required to provide Support Services in the provision of the Attack Surface Management Offering, Darktrace shall be a Data Processor and the Data Processing Agreement available at https://darktrace.com/legal/master-services-agreement shall apply.

4.3. Customer warrants and represents to Darktrace that it has all necessary consents, authorizations and legitimate purposes in order to provide Darktrace with the Personal Data under this Prevent Schedule, and shall indemnify Darktrace from and against any third party claims arising out of or in relation to the transfer of Personal Data from Customer to Darktrace.

DARKTRACE

SCHEDULE 2: Darktrace / Incident Readiness & Recovery

This Schedule (the "**IRR Schedule**") is applicable where Customer has purchased the **Darktrace Incident Readiness & Recovery** product offering (the "**Incident Readiness & Recovery Offering**").

1. ACCESS TO AND USE OF THE OFFERING

1.1. Customer's use of the Incident Readiness & Recovery Offering, and Darktrace's delivery of the Incident Readiness & Recovery Offering, is provided subject to the terms of the Agreement.

2. DELIVERY OF THE OFFERING

2.1. Where the Incident Readiness & Recovery Offering user interface (the "**Incident Readiness & Recovery UI**") is integrated with third party software tools ("**Third Party Tools**"), such that actions in Third Party Tools are triggered via the Incident Readiness & Recovery UI ("**Incident Readiness & Recovery UI Actions**"), Customer acknowledges and agrees that Customer shall be solely responsible for any effect, result or outcome of taking any Incident Readiness & Recovery UI Action. Under no circumstances shall Darktrace be liable to Customer for the consequences of a Incident Readiness & Recovery UI Action taken by Customer, Customer Affiliates, Outsource Providers, sub-contractors, agents or any third parties.

2.2. Customer acknowledges and agrees that it is responsible for determining which users of the Incident Readiness & Recovery Offering is granted the applicable permissions to access Incident Readiness & Recovery UI Actions.

2.3. Where Customer configures the Incident Readiness & Recovery Offering to generate simulated cyber incidents to appear on the Incident Readiness & Recovery UI ("**Simulated Incidents**"), Customer acknowledges and agrees that Customer shall be solely responsible for any act, measure or process entered into outside of the Incident Readiness & Recovery UI in response to a Simulated Incident. Under no circumstances shall Darktrace be liable in any respect for any action taken in a live environment, or otherwise, in response to a Simulated Incident.

3. WARRANTIES

3.1. Darktrace provides no warranties or representations as to the accuracy or reliability of the data, analysis, or recommendations generated by the Incident Readiness & Recovery Offering and any conclusions, decisions, actions or interpretations of the data provided by the Incident Readiness & Recovery Offering are inferred or taken at Customer's own risk. To the fullest extent permissible by applicable law, Darktrace accepts no liability for any actions taken or inferences made by Customer pursuant to the provisions of this clause 3.1.

3.2. Customer warrants and undertakes that, unless otherwise specified in a Product Order Form, in the event that Customer expands its Darktrace / NETWORK deployment, Customer shall pay Darktrace's then-current standard fees for the corresponding expansion in deployment of the Incident Readiness & Recovery Offering.

4. DATA PROTECTION

4.1. In the event that Darktrace is required to provide Support Services in the provision of the Incident Readiness & Recovery Offering, Darktrace shall be a Data Processor and the Data Processing Agreement available at https://darktrace.com/legal/master-services-agreement shall apply.

DARKTRACE

SCHEDULE 3: Darktrace / CLOUD

This Schedule (the "**Cloud Schedule**") is applicable where Customer has purchased the **Darktrace / CLOUD** product offering (the "**Cloud Offering**").

1. ACCESS TO AND USE OF THE OFFERING

1.1. Customer's use of the Cloud Offering, and Darktrace's delivery of the Cloud Offering, is provided subject to the terms of the Agreement.

2. DELIVERY OF THE OFFERING

2.1. The Cloud Offering is provided as a distinct product offering to any product or service provided under Darktrace's pre-existing product and services range.

2.2. Customer acknowledges that, whilst the Cloud Offering may be deployed without agents, installing agents into the applicable Customer cloud environment (the "**Customer Environment**") may result in improved visibility and coverage over traffic and architecture within the Customer Environment.

2.3. Customer acknowledges that the integration of the Cloud Offering into the Customer Environment may result in increased cloud hosting and transfer fees and agrees to accept sole responsibility for any such increases. Under no circumstances shall Darktrace be directly or indirectly liable for any such increases.

3. WARRANTIES

3.1. Darktrace provides no warranties or representations as to the accuracy or reliability of the data generated by the Cloud Offering and any conclusions, decisions, actions or interpretations of the data provided by the Cloud Offering, including in relation to suggestions provided by the Cloud Offering itself, are inferred or taken at Customer's own risk. To the fullest extent permissible by applicable law, Darktrace accepts no liability for any actions taken or inferences made by Customer pursuant to the provisions of this clause 3.1.

3.2. The Cloud Offering is provided as a supplementary tool for Customer's security and compliance teams and the Cloud Offering is not a complete substitute for human intervention. Darktrace accepts no liability, for any reason, for: (i) Customer being non-compliant with any law, regulation or court order; (ii) how Customer determines to utilize or prioritize its security resources or time; or (iii) any disruption, delay or damage caused directly or indirectly as a result of response actions taken by Cloud Offering.

4. DATA PROTECTION

4.1. In the event that Darktrace is required to provide Support Services in the provision of the Cloud Offering, Darktrace shall be a Data Processor and the Data Processing Agreement available at https://darktrace.com/legal/master-services-agreement shall apply.

DARKTRACE

SCHEDULE 4: Darktrace / Forensic Acquisition & Investigation

This Schedule (the "**FAI Schedule**") is applicable where Customer has purchased the **Darktrace / Forensic Acquisition & Investigation** product offering (the "**FAI Offering**").

1. ACCESS TO AND USE OF THE OFFERING

1.1. Customer's use of the FAI Offering, and Darktrace's delivery of the FAI Offering, is provided subject to the terms of the Agreement.

1.2. The FAI Offering was previously named Cado Security Software. This schedule also applies for Customers who have purchased the FAI Offering under the name Cado Security Software.

2. DELIVERY OF THE OFFERING

2.1. Where the FAI Offering is provided as an Evaluation Offering, Parties acknowledge that the FAI Offering is not intended to house or contain any sensitive or commercial data. Darktrace shall not be liable or responsible under any circumstances for any sensitive or commercial data input into such environment by Customer or any resulting loss or damage thereto.

2.2. Customer will be solely responsible for installing any updates and modifications that Darktrace may make available from time to time. Darktrace will only provide FAI Support Services (as defined below) for the most recent version of the FAI Offering.

2.3. Support Services are not provided in relation to the FAI Offering. Darktrace provides basic support via the customer portal for the FAI Offering that is accessible at https://support.cadosecurity.com (the "**FAI Support Service**").

2.4. Darktrace may collect, process, aggregate, and use certain information, analysis, statistics, and other data generated by Customer's use of the FAI Offering (a) to confirm that the FAI Offering is being used in accordance with the rights granted under this Agreement, and (b) to drive improvements in the FAI Offering. Darktrace will retain ownership of such FAI Offering usage data.

3. WARRANTIES

3.1. For the purposes of providing the FAI Offering, "Product Specifications" as referred to by the Software Warranty, shall be defined as the technical documentation outlining the performance of the FAI Offering made available at https://support.cadosecurity.com.

4. DATA PROTECTION

4.1. In providing the FAI Support Service and/or Darktrace collects use data in relation to the provision of the FAI Offering, Darktrace shall be a Data Processor and the Data Processing Agreement available at https://darktrace.com/legal/master-services-agreement shall apply.

DARKTRACE

SCHEDULE 5: DARKTRACE LABS

This Schedule (the "**Darktrace Labs Schedule**") is applicable to any Customer using or accessing the Darktrace Labs product offering (the "Darktrace Labs Offering").

1. ACCESS TO AND USE OF THE OFFERING

1.1. Customer's use of the Darktrace Labs Offering, and Darktrace's delivery of the Darktrace Labs Offering, is provided subject to the terms of the Agreement.

2. DELIVERY OF THE OFFERING

2.1. The Darktrace Labs Offering is a distinct product offering to any product or service provided under Darktrace's pre-existing product and services range.

2.2. Customer is permitted to use the Darktrace Labs Offering only for the purpose of non-production testing, training and demonstration of the Darktrace product suite.

2.3. In addition to the restrictions contained in Clause 4.6 of the Agreement, Customer shall not use the Darktrace Labs Offering:

2.3.1. to publish, send, or facilitate the sending of unsolicited electronic messages;

2.3.2. to run any malware without the prior written consent of Darktrace;

2.3.3. in relation to any DDOS or other cyber attack;

2.3.4. in relation to any activity that promotes or facilitates child sexual exploitation or abuse;

2.3.5. to threaten, incite, or encourage violence, terrorism, or other harm;

2.3.6. to violate or attempt to violate the rights of any third party;

2.3.7. to mine for cryptocurrency; or

2.3.8. to cause, encourage or assist any third party to do any of the foregoing.

2.4. Customer may not use any content uploaded or produced using the Darktrace Labs Offering in a production, live, or commercial setting.

2.5. Any software vulnerabilities or defects that are detected in the Darktrace Labs Offering by Customer shall be notified to Darktrace in writing promptly, and in any event, within 20 days of Customer's discovery of such vulnerability or defect.

2.6. Darktrace may collect, process, aggregate, and use certain information, analysis, statistics, and other data generated by Customer's use of the Darktrace Labs Offering (a) to confirm that the Darktrace Labs Offering is being used in accordance with the rights granted under the Agreement and the Darktrace Labs Schedule, and (b) to drive improvements in the Darktrace Labs Offering. Darktrace will retain ownership of such usage data.

2.7. Customer availability of the Darktrace Labs Offering is subject to available Darktrace Labs usage credits, and these credits may be issued, modified, suspended or revoked at Darktrace's sole discretion and without prior notice. Darktrace does not guarantee any level of Darktrace Labs availability or credit allocation to Customer.

3. TERMINATION

3.1. In addition to the provisions of the Agreement, in the event that Darktrace in its sole discretion suspects any breach of the conditions in Clause 2.3 above, Darktrace may immediately and without notice suspend Customer's access to the Darktrace Labs Offering and permanently delete or destroy all and any associated content.

3.2. In the event that Darktrace terminates the Agreement in connection with Customer's use of the Darktrace Labs Offering under Clause 12.2 of the Agreement, notwithstanding the provisions of Clause 12.4 of the Agreement, Darktrace shall have no obligation to store or return any data of Customer stored or hosted within the Darktrace Labs Offering.

4. INDEMNITY

4.1. Customer shall indemnify, defend and hold harmless Darktrace (and its affiliates, officers, directors, shareholders, employees, consultants, and agents, together the "Darktrace Indemnitees") from all losses, liabilities, damages, costs and expenses (including without limitation reasonable attorneys' fees, expert witness fees and court costs) in respect of any claim, action, suit or proceeding brought by third parties ("Claim") that arises out of or in connection with (i) Customer's use of the Darktrace Labs Offering; (ii) Customer's breach of the Agreement or the Darktrace Labs Schedule; (iii) Customer's violation of third party rights or Applicable Laws related to use of the Darktrace Labs Offering; or (iv) any content uploaded or created within the Darktrace Labs Offering. Customer will not enter into any settlement or compromise of any such Claim without Darktrace's prior written consent.

4.2. The exclusions and limitation on liability in Clause 11 of the Agreement shall not apply to the Darktrace Labs Schedule.

5. NO WARRANTY

5.1. Darktrace provides no warranties or representations as to the accuracy or reliability of the data generated by the Darktrace Labs Offering and any conclusions, decisions, actions or interpretations of the data provided by the Darktrace Labs Offering are inferred or taken at Customer's own risk. To the fullest extent permissible by applicable law, Darktrace accepts no liability for any actions taken or inferences made by Customer pursuant to the provisions of this Clause.

6. DATA PROTECTION

6.1. In providing Support Services and/or collecting use data in relation to the provision of the Darktrace Labs Offering, Darktrace shall be a Data Processor and the Data Processing Agreement available at https://darktrace.com/legal/master-services-agreement shall apply.

DARKTRACE

SCHEDULE 6: Darktrace / SECURE AI

This Schedule (the "**Secure AI Schedule**") is applicable where Customer has purchased the **Darktrace / SECURE AI** product offering ("**Secure AI**").

1. ACCESS TO SECURE AI

1.1. Customer's use of Secure AI, and Darktrace's delivery of Secure AI, is provided subject to the terms of the Agreement and as a distinct product offering to any product or service provided under Darktrace's pre-existing product and services range.

2. DELIVERY AND USE OF SECURE AI

2.1. In addition to the usage restrictions set out in the Agreement, Customer's use of Secure AI is subject to the Acceptable Use Policy set out below, and any breach of the Acceptable Use Policy shall be considered a breach for the purposes of the Agreement.

2.2. Customer exclusively determines the purposes and means of any monitoring, searching, modelling, profiling, policy enforcement, and other analysis performed using Secure AI, including: (a) which data sources are connected; (b) what prompts, logs, messages or content are collected or uploaded; (c) the scope, rules, policies, thresholds, alerts, and models applied; and (d) whether and how Secure AI outputs are used in relation to any individual.

2.3. Customer is solely responsible for ensuring that its use of Secure AI (including its configuration, any policies it converts into models, and any outputs or alerts acted upon) complies with all applicable privacy, employment, monitoring, communications, workplace, and data protection laws and regulatory guidance. Without limiting the foregoing, Customer acknowledges that is solely liable for:

2.3.1. establishing and documenting an appropriate lawful basis (and, where required, satisfy conditions for processing special category data) for processing Customer Data;

2.3.2. providing all required notices and transparency information to employees and other individuals whose Personal Data is processed, including in relation to monitoring and automated analysis;

2.3.3. obtaining all required consents and/or approvals (including, where applicable, works council/employee representative or trade union consultation/agreements) and maintaining evidence of the same;

2.3.4. conducting and documenting any required data protection impact assessment(s), legitimate interest assessment(s), risk assessments, and implementing appropriate safeguards, including in respect of employee monitoring, profiling and/or automated decision-making;

2.3.5. ensuring that access to Customer Data and outputs is appropriately restricted to authorized personnel on a need-to-know basis, and that appropriate retention and deletion settings are implemented and maintained; and

2.3.6. ensuring that any decisions or actions taken based on Secure AI outputs, alerts, or models comply with applicable law, including any requirements for human review, proportionality, and non-discrimination.

3. WARRANTIES AND DISCLAIMERS

3.1. Customer is solely responsible for its use of Secure AI, the activities of its users and for the accuracy, integrity, legality, reliability and appropriateness of all Customer Data. Customer expressly recognizes that Darktrace does not create nor endorse any Customer Data processed by or used in conjunction with Secure AI. Customer acknowledges that it is fully and solely responsible for its own Customer Data and all contents within the Customer Data, and will, at Customer's own expense, indemnify, defend and hold Darktrace, its Affiliates, and their respective officers, directors, and employees, ("Darktrace Indemnitees") harmless from and against all liabilities, damages, and costs, including settlement costs and reasonable attorneys' fees, incurred by reason of Darktrace's compliance with the instructions of Customer with respect to the ownership, custody, processing or disposition of the Customer Data by Darktrace, as applicable.

3.2. Customer assumes all liability for, and shall defend, indemnify and hold harmless Darktrace Indemnities from and against, any and all claims, demands, proceedings, regulatory investigations or enforcement actions, fines, penalties, damages, losses, costs and expenses (including reasonable legal fees) arising out of or in connection with: (a) Customer's use of Secure AI in breach of applicable law or this Addendum; (b) Customer's failure to provide required notices, obtain required consents/approvals, or complete required assessments; (c) Customer's configuration of Secure AI or instructions to Darktrace, including the selection of data sources, retention, access controls, policies and models; and/or (d) any decision, disciplinary measure, employment action or other action taken by Customer or its users based on Secure AI outputs.

3.3. Darktrace provides no warranties or representations as to the accuracy or reliability of the data generated by Secure AI and any conclusions, decisions, actions or interpretations of the data provided by Secure AI, including in relation to suggestions provided by Secure AI itself, are inferred or taken at Customer's own risk. To the fullest extent permissible by applicable law, Darktrace accepts no liability for any actions taken or inferences made by Customer pursuant to the provisions of this clause 3.3. Secure AI is provided as a supplementary tool for Customer's security and compliance teams and Secure AI is not a complete substitute for human intervention. Darktrace accepts no liability, for any reason, for: (i) Customer being non-compliant with any law, regulation or court order; (ii) how Customer determines to utilize or prioritize its security or AI resources or time; or (iii) any disruption, delay or damage caused directly or indirectly as a result of response actions taken by Secure AI.

4. ACCEPTABLE USE POLICY

4.1. Customer's use of the Offering must follow usage policies set out in this section (together, the "Acceptable Use Policy").

4.2. The Offering shall not be used for the proliferation or enactment of harm. The Offering may never be used in furtherance of:

4.2.1. threats, intimidation, harassment, or defamation;

4.2.2. illicit activities, goods, or services;

4.2.3. destruction, compromise, or breach of another's system or property, including malicious or abusive cyber activity or attempts to infringe on intellectual property rights of others;

4.2.4. provision of tailored advice that requires a license, such as legal or medical advice, without appropriate involvement by a licensed professional; or

4.2.5. circumventing our safeguards.

4.3. The Offering shall not be used for unlawful invasion of privacy, including to aggregate, monitor, profile, or distribute individuals' private or sensitive information without their authorization. The Offering may never be used for:

4.3.1. facial recognition databases without data subject consent;

4.3.2. real-time remote biometric identification in public spaces;

4.3.3. use of someone's likeness, including their photorealistic image or voice, without their consent in ways that could confuse authenticity;

4.3.4. evaluation or classification of individuals based on their social behavior, personal traits, or biometric data (including social scoring, profiling, or inferring sensitive attributes);

4.3.5. inference regarding an individual's emotions in the workplace and educational settings, except when necessary for medical or safety reasons; or

4.3.6. assessment or prediction of the risk of an individual committing a criminal offense based solely on their personal traits or on profiling.

4.4. The Offering shall not be used to manipulate or deceive people, to interfere with their exercise of human rights, to exploit people's vulnerabilities, or to interfere with their ability to get an education or access critical services, including any use for:

4.4.1. deceit, fraud, scams, spam, or impersonation;

4.4.2. political campaigning, lobbying, foreign or domestic election interference, or demobilization activities; or

4.4.3. automation of high-stakes decisions in sensitive areas without human review: (a) critical infrastructure; (b) education; (c) housing; (d) employment; (e) financial activities and credit; (f) insurance; (g) legal; (h) medical; (i) essential government services; (j) product safety components; (k) national security; (l) migration; or (m) law enforcement.

4.5. The Offering shall not be used any other use for which use of AI is not permitted under applicable law or regulation.