

**APPENDIX 4:
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 Term), 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.

SCHEDULE 2: Darktrace / Incident Readiness & Recovery

This Schedule (the “Heal 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 DETECT™ 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.

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.