**RANSOMWARE RESPONSE SERVICE ADDENDUM**

The terms set forth in this Ransomware Response Service Addendum (this "**Addendum**") govern Absolute's standard offering for ransomware response service for the Absolute Products, as revised from time to time ("**Ransomware Response Service**"), if the Ransomware Response Service is included in the edition of the Absolute Products purchased by Customer under an Order Form or is otherwise purchased by Customer under an Order Form. Capitalized terms used but not defined in this Addendum have the meanings given to them in the Absolute Products Addendum available at https://www.absolute.com/company/legal/agreements/absolute/visibility-control-and-resilience-product-addenda or if not defined in the Absolute Products Addendum, then the Master Subscription Agreement or other agreement between Customer and Absolute governing Absolute's provision of the Absolute Products to Customer (the "**Agreement**"). The Ransomware Response Service constitutes Services for the purposes of the Agreement.

**1. Definitions**.

**"Incident Manager"** means a named individual from Customer's security team who will act as Absolute's primary contact for the Ransomware Response Service.

**"Incident Manager Contact Information"** means, with respect to the Incident Manager, the first and last name, title, email address, phone number and mobile phone number.

**"Infected Device"** means a Device that is infected with Ransomware.

**"Quarantine"** means executing a script on an Infected Device for the purposes of enabling Windows Firewall and blocking inbound and outbound network communications except to the Hosted Service or such other 3rd party services as may be explicitly "whitelisted" (e.g., to enable a third-party Endpoint Protection ("**EPP**") or Endpoint Management ("**EMM**") application to communicate with its associated services).

**"Ransomware"** means malicious third-party software that infects a Device and renders it inoperable through means that may include but not be limited to encryption of data stored on the Device for the purpose of extracting a payment (i.e. ransom) in exchange for restoration of such Device's operability.

**"Ransomware Incident"** means the compromise of one (1) or more Infected Devices by a particular Ransomware instance.

**"Ransomware Response Actions"** means one or more instances of actions performed on a Device for the purposes of: (i) identifying whether it is an Infected Device; (ii) executing one or more scripts; (iii) performing a Device Freeze Operation; (iv) by performing end user messaging via the Hosted Service; and/or (v) performing repair or reinstall operations for one or more applications (provided, however, that such applications and their applicable versions must be enabled for Application Persistence prior to the Ransomware Incident).

**"Ransomware Response Period"** means the thirty (30) day period commencing on the date of Customer's written notice to Absolute of the occurrence of a Ransomware Incident for which it wishes Absolute to perform an instance of the Ransomware Response Service.

**"Ransomware Response Readiness Assessment"** means the initial assessment of Customer's readiness for a Ransomware Incident as performed by Absolute upon purchase of the Ransomware Response Service. Such assessment may identify actions that Customer must perform prior to and as a condition of Absolute's subsequent performance of an instance of the Ransomware Response Service (e.g., including but not limited to deploying and/or updating its EPP and/or EMM applications to specified versions, or enabling Application Persistence for such versions for all Devices. Customer agrees and acknowledges that failure to perform such actions in a timely fashion shall entitle Absolute, in its sole and absolute discretion, to reject performance of the Ransomware Response Service.

**"Recovery"** means the restoration of an Infected Device to an operable state through removal of the Ransomware, repair and/or reinstall of the Customer's designated EPP and EMM application(s) as applicable, and removal of the Device from Quarantine. For avoidance of doubt, successful Recovery: (i) may be based on re-imaging the Device as means of Ransomware removal; and (ii) does not require that all of the Device's data be restored as a condition of Recovery; and (iii) Absolute shall not be responsible for any loss of data or for providing or performing any data backup or restoration services or operations.

**2. Ransomware Response Activation Requirements.** In order to be eligible to activate the Ransomware Response Service: (i) all of Customer's active Subscriptions must include the Ransomware Response Service; (ii) Customer must have completed the Ransomware Response Readiness Assessment; and (iii) Customer shall not have exceeded two (2) Ransomware Incidents in the preceding 12-month period.

**3. Ransomware Response Activation.** Not more than twice per 12-month period during the Subscription Term (unless separately agreed to by Absolute in writing under a statement of work, which will involve additional Professional Services fees), Customer may activate the Ransomware Response Service by submitting a request in writing to Absolute's Support Services team. Upon Absolute's receipt of Customer's request and Absolute's written confirmation of Customer's eligibility (each such confirmed request a "**Ransomware Response Order**"), and subject to the terms set forth herein (including Customer meeting the requirements in Section 4, below), Absolute will use commercially reasonable efforts for the Ransomware Response Period to identify, Quarantine, and assist in the recovery of Infected Device(s) by performing the Ransomware Response Service and Customer agrees to fully cooperate with such efforts.

**4. Customer Obligations.** Within twenty-four (24) hours of any Ransomware Response Order, Customer agrees to provide Absolute with: (i) a designated Incident Manager and Incident Manager Contact Information; (ii) all available information on the Ransomware Incident (e.g., including but not limited to the name, location, and hashes of its associated files); (iii) all available information on Infected Devices (to the extent then-currently known), including but not limited to Device serial numbers, or other Device identifying information; and (iv) such reasonable administrative access as may be required by the Hosted Service for the purpose of assisting Customer in performing actions necessary to effect Recovery.

**5. Ransomware Response Limitations.** Customer acknowledges and agrees that:

a) the Ransomware Response Service may be limited or unavailable, and Absolute will have no obligations under this Addendum, with respect to an Infected Device in the following circumstances: (i) the Infected Device does not contact the Hosted Service pre-incident or post-incident; (ii) a service or feature has been previously launched on the Infected Device (for example, a Data Delete Operation or a Device Freeze Operation) that restricts or disables the ability of the Infected Device to contact the Hosted Service; or (iii) the Infected Device does not have a valid Subscription with the Ransomware Response Service.

b) RECOVERY OF EVERY INFECTED DEVICE CANNOT BE GUARANTEED. WITHOUT LIMITING THE GENERALITY OF THE FOREGOING, NO GUARANTEE OR WARRANTY IS PROVIDED WITH RESPECT TO THE ABILITY TO RECOVER AN INFECTED DEVICE. ABSOLUTE WILL NOT BE RESPONSIBLE FOR ANY DAMAGE TO AN INFECTED DEVICE OR LOSS OF DATA THAT OCCURS DURING ITS PERFORMANCE OF THE RANSOMWARE RESPONSE SERVICE, INCLUDING WITHOUT LIMITATION, DAMAGE CAUSED BY THIRD-PARTY RANSOMWARE TO CUSTOMER'S SYSTEMS OR DATA. OTHER THAN AS EXPRESSLY SET FORTH IN THIS ADDENDUM, ABSOLUTE DOES NOT GUARANTEE, AND MAKES NO REPRESENTATIONS OR WARRANTIES CONCERNING, ITS PERFORMANCE OF THE RANSOMWARE RESPONSE SERVICE WITH RESPECT TO ANY DEVICE.

*****