DEVICE THEFT INVESTIGATION AND RECOVERY SERVICES ADDENDUM

The terms set forth in this Device Theft Investigation and Recovery Services Addendum (this "**Addendum**") govern Absolute's standard offering for device theft investigation and recovery services for the Absolute Products, as revised from time to time ("**Device Theft Investigation and Recovery Services**"), if the Device Theft Investigation and Recovery Services are included in the edition of the Absolute Products purchased by Customer under an Order Form or are 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 Device Theft Investigation and Recovery Services constitute Services for the purposes of the Agreement.

1. Definitions.

"**Forced Re-Enrollment Feature**" refers to the device setting in Chromebooks that allows administrators to force Devices to be re-enrolled to their original Google administrator's console, even after a Device is wiped.

"**Google Management Console**" means the web-based management console available from Google Inc. for managing Chromebooks.

"**Incident Date**" means the first date on which Customer becomes aware of the theft, or could reasonably be expected to discover the theft, of a Stolen Device.

"**Incident Report Date**" means the date of actual receipt by Absolute of a fully-completed Investigation Report (including details of the Official Report).

"**Investigation Report**" means the form provided by Absolute and available to Customer either by (a) logging into the Customer account accessible via the Hosted Service, or (b) requesting the form to be mailed to Customer by using the contact information available through customer support. If Customer is a managed services provider, the Investigation Report must be completed and submitted to Absolute by Customer, not by its MSP End Users.

"**Official Report**" means an official police report and any other form required by the law enforcement authority required to report the theft of a Device.

"**Post-Incident Data**" means data generated by a Stolen Device or obtained from third parties after the theft of a Stolen Device and during a theft recovery, including data created and stored by users having possession of or access to a Stolen Device after its loss, data that is accessed or modified by such users and data collected and stored by Apple Inc. or Google Inc. Post-Incident Data includes, without limitation, information obtained by utilizing any and all of Absolute's theft recovery tools in order to recover Stolen Device(s) to the extent permitted by applicable laws.

"**Recover**", "**Recovered**" or "**Recovery**" means a Stolen Device has been located and returned to Customer, or is in the process of being delivered to Customer, or is either in possession of, or in the process of being collected by or actively tracked by, law enforcement.

"**Restricted Loss**" means any of the following with respect to a Stolen Device:

(a) the theft was materially facilitated by Customer's criminal acts, gross negligence or wilful misconduct when securing the Stolen Device in question, or the repeated theft of Stolen Devices demonstrates a pattern of any such criminal, negligent or wilful activity;

(b) the law enforcement authority in the jurisdiction in which the Stolen Device went missing does not consider the theft to be a criminal act;

(c) the theft of the Stolen Device was intentional, or was part of a Theft Detection Program, or Customer fails to fully complete the Investigation Report form;

(d) if the Stolen Device is a Chromebook, Customer has not purchased the Google Management Console and used it on the Stolen Device to deploy the current Absolute for Chromebooks extension;

(e) if the Stolen Device is a Chromebook, Customer has not upgraded the Stolen Device to a version that is capable of supporting Google's Forced Re-Enrollment Feature for the edition of the Absolute Products purchased by Customer and enabled Google's Forced Re-Enrollment Feature within thirty (30) days of it becoming available;

(f) the Software was not installed or not activated on the Stolen Device prior to the Incident Date; or

(g) the Stolen Device was not stolen (as reasonably determined by Absolute).

"**Stolen Device**" means a Device for which an Investigation Report has been submitted to Absolute in respect of the theft of such Device.

"**Theft Detection Program**" means any intentional loss or investigative program or operation, instigated, orchestrated, contributed to or carried out by or on behalf of Customer with or without the assistance of law enforcement, where the purpose of such operation in whole or in part is to attract theft or loss for the purpose of identifying or apprehending thieves or other wrongdoers.

"**Theft Recovery Territory**" means any region or country, except where:

(a) Absolute has indicated such region or country as being excluded, or

(b) in Absolute's sole discretion, such region or country is not a region or country in which (i) the culture, customs and actual governance include an adherence to the rule of law, (ii) there are presently governmental resources that are reasonably required to enforce the laws therein, (iii) the infrastructure supports unimpeded transmission of the data required for tracking and recovery purposes, (iv) tracking and investigative activities are not prohibited by applicable laws, and (v) in the case of the Stolen Device moving between multiple jurisdictions, the policing bodies of both jurisdictions collaborate in the enforcement of their respective property laws.

2. Consent. By activating the Device Theft Investigation and Recovery Services, including by filing an Investigation Report in respect of a Stolen Device, Customer authorizes and instructs Absolute to: (a) coordinate with local law enforcement officials to recover the Stolen Device, (b) access and collect any information about the Stolen Device held by third parties, including by accessing Customer's Google account to obtain information relating to the Stolen Device, and Customer agrees to facilitate access to such information by Absolute; (c) in Absolute's discretion, initiate, activate, de-activate or cancel a Device Freeze Operation, if available, in order to assist with the theft recovery process, (d) access Post-Incident Data on the Stolen Device or in the control of third parties solely for the purpose of performing the theft recovery, where any such Post-Incident Data will be stored on a secure server and will only be divulged to police investigators or official prosecutors involved in the investigation or prosecution of the criminal offence related to the loss of the Stolen Device, and (e) transfer any data gathered in the course of a theft recovery (including Post-Incident Data) to the applicable criminal justice system, including law enforcement personnel, prosecutors and courts, and acknowledge that such data in connection with a theft recovery will be made available to Customer only at the discretion of these criminal justice system entities. If Customer is a managed services provider, Customer must obtain authorization from its applicable MSP End Users for Absolute to do the foregoing.

3. No Theft Recovery Outside of Territory. The Device Theft Investigation and Recovery Services are available only in the Theft Recovery Territory. If the contact from the Stolen Device after the Incident Report Date originates from outside of the Theft Recovery Territory, the Device Theft Investigation and Recovery Services are no longer available and are replaced by the Remote Wipe and Lock Functionality, and a successful activation of the Remote Wipe and Lock Functionality (of any type) or Customer's decision not to activate the Remote Wipe and Lock Functionality fulfills any applicable Device Theft Investigation and Recovery Services obligation of Absolute.

4. Obligations for Theft Recovery. Upon Customer's activation of the Device Theft Investigation and Recovery Services, Absolute will use commercially reasonable efforts to locate and Recover the Stolen Device and Customer agrees to fully cooperate with such efforts. From time to time Customer will be informed of the status of the effort to Recover the Stolen Device through e-mail or online through the Hosted Service. Subject to Section 3 above, Customer further agrees that Absolute will only have an obligation to actively pursue Recovery (a) for a period of one year from the Incident Report Date, or (b) until the date that the Remote Wipe and Lock Functionality is activated for the Missing Device, whichever is earlier.

5. Theft Recovery Activation. Customer acknowledges that the likelihood of Recovery decreases the further the Incident Report Date is from the Incident Date. Accordingly, in order to activate the Device Theft Investigation and Recovery Services, Customer must as quickly as possible but in any event no later than fourteen (14) days after the Incident Date:

(a) report the Stolen Device as stolen to the law enforcement authority in the jurisdiction in which the Stolen Device was stolen by completing and submitting an Official Report to such authority;

(b) obtain a record or identifying number (such as the police or other file number) of the Official Report, and at the request of Absolute, a copy of the Official Report; and

(c) duly complete and submit an Investigation Report to Absolute, ensuring that such Investigation Report contains such details of the Official Report as are required by Absolute.

6. Limitations. Customer acknowledges and agrees that Absolute's obligation and ability to successfully Recover any Stolen Device will be substantially and materially reduced if:

(a) the theft or loss of a Stolen Device is a Restricted Loss; or

(b) a Stolen Device is a device that is not capable of supporting persistence for the edition of the Absolute Products purchased by Customer or on which persistence was not enabled at the time of the theft. Persistence is not required for Chromebooks; however, if a Stolen Device is a Chromebook, and if a version of Chrome OS becomes available that is capable of supporting Google's Forced Re-Enrollment Feature for the edition of the Absolute Products purchased by Customer, within thirty (30) days of such version becoming available Customer must have upgraded the Stolen Device to that version and enabled Google's Forced Re-Enrollment Feature; if Customer fails to do so, the theft of the Stolen Device will be a Restricted Loss. A list of devices that are capable of supporting persistence is available from Absolute.

7. Theft Recovery Preventions and Other Features. Customer acknowledges and agrees that:

(a) the Device Theft Investigation and Recovery Services may be ceased by Absolute, and all applicable obligations of Absolute under this Addendum will be deemed satisfied, when the Remote Wipe and Lock Functionality has been activated on a Stolen Device,

(b) the Stolen Device must be enrolled in Customer's account with the Hosted Service prior to the earlier of (i) the Incident Date and (ii) 30 days before the date of theft reported on an Investigation Report, and must not be unenrolled until such Stolen Device is returned to Customer's possession or Recovered, and

(c) RECOVERY OF EVERY STOLEN DEVICE CANNOT BE GUARANTEED. WITHOUT LIMITING THE GENERALITY OF THE FOREGOING, (I) AS ABSOLUTE WILL ONLY COORDINATE RECOVERIES IN A THEFT RECOVERY TERRITORY, NO GUARANTEE OR WARRANTY IS PROVIDED WITH RESPECT TO THE OPERATION OF THE ABSOLUTE PRODUCTS, OR THE ABILITY TO RECOVER A STOLEN DEVICE USING THE ABSOLUTE PRODUCTS, IF THE STOLEN DEVICE IS LOCATED OR MOVED OUTSIDE OF THE THEFT RECOVERY TERRITORY; (II) ABSOLUTE'S DEVICE THEFT INVESTIGATION AND RECOVERY SERVICES ARE SUBJECT TO AND CONDITIONED ON THE CONTINUED INTEROPERABILITY BETWEEN THE ABSOLUTE SERVICE AND THE STOLEN DEVICE, INCLUDING, WITHOUT LIMITATION, THE STOLEN DEVICE'S OPERATING SYSTEM AND (III) CUSTOMER ACKNOWLEDGES AND AGREES THAT FOR PURPOSES OF THE DEVICE THEFT INVESTIGATION AND RECOVERY SERVICES, "STOLEN DEVICES" DOES NOT INCLUDE ANY APPLE INC. MANUFACTURED DEVICES.

* * * * *