VERITAS™

HOSTED SERVICES ADDENDUM

Customer Company Name:	**General Services Administration** **Ordering Activity**
Title and/or Effective Date of Master Agreement:	Master License Agreement GSA Schedule
Veritas Agreement Number (VAN) of Primary Agreement: **Veritas Agreement Number (VAN) of this Addendum:**	MLA110631.01 HSA VAN CLD126860.01
"Effective Date" of this Addendum:	August 20, 2024

This Addendum is entered into by and between the Customer identified above ("**Customer**"), and Veritas, defined as each of the Veritas entities signing this Addendum (individually, "**Veritas**"), under the Primary Agreement referenced above ("**Agreement**"), the terms of which are incorporated by reference.

The following Hosted Services terms shall supplement the terms of the Agreement:

Customer and Veritas agree to amend the Agreement as follows solely with respect to Customer's purchase, and Veritas' delivery, of any services Veritas classifies as "hosted", "software-as-a-service", or "cloud" services ("Service(s)").

1. The following definitions are hereby added to the Agreement:

a) "**Actual Use Level**" means Customer's actual quantity, type and duration of Service use, regardless of Registered Use Level.

b) "**Certificate"** means the machine-generated certificate sent to Customer by Veritas to confirm a purchase of the applicable Service, whether ordered directly from Veritas or through Veritas' authorized channel partner.

c) "**Customer Data**" means information which the Customer uploads to the Service to be processed and/or stored through the Service.

d) "**Provisioning Information"** means information that Veritas needs to configure the Service, and/or to provide any included support for the Service to the Customer, including but not limited to, names, e-mail address, IP address and contact details of designated users and contacts for the Service, and other Personal Information provided during configuration of the Service or any subsequent support call.

e) "**Entitlement**" means Customer's right to access, use and/or benefit from, a given Service.

f) "**Initial Period**" means the initial minimum period of time for which Customer commits to subscribe to and pay for a Service, as set forth in a Service Order.

g) **"Personal Information"** means information from which a living individual can be recognized.

h) "**Registered Use Level**" means the quantity and type of Entitlements for which Customer is committed to pay. Registered Use Level may also be referred to as the Minimum Contracted Quantity.

i) "**Renewal Period**" means each of the subsequent, sequential Service periods following the Initial Period.

j) "**Service(s)**" means cloud-based and/or hosted Veritas service(s), sold to Customer hereunder, whether as an individual service or as a collective bundle of related services, including any Service Components.

k) “**Service Component**” means certain enabling software, hardware peripherals and associated documentation which may be separately provided by Veritas as an incidental part of a Service.

l) “**Service Description**” means Veritas’ standard, then-current description of a Service’s features, including any product-specific additional terms and requirements, and any accompanying service level targets (“**SLA**”), if applicable. Current copies of all Service Descriptions are available at https://www.veritas.com/about/legal/license-agreements. For clarity, if an Ordering Activity places its order for Service(s), then, such Ordering Activity, upon request, will be provided with the Service Description for review at the time it places an order.

m) “**Service Meter**” sometimes called, “**Use Level**” means the applicable unit(s) of measurement by which Veritas prices and sells an Entitlement to a Service, in effect at the time the relevant Service Order is created. (For example, “per device” or “1GB per User” or “per X” each could be Service Meters for given services).

n) “**Service Order**” means the Parties’ mutually agreed commitment for a Service or Services under this Addendum. A Service Order may take the form of a written addendum, exhibit or statement of work signed by the Parties, or in the absence of such a document, Customer’s order accepted by Veritas directly or through an authorized Veritas channel partner, as documented in the Certificate issued in confirmation of such order.

o) “**Term**” means, for a given Service, the Initial Period together with any Renewal Periods.

2. **ORDERING.** Veritas reserves the right to indicate the method(s) by which it will receive and accept orders for a given Service.

3. **SERVICE.** Veritas agrees to provide the Service specified in the Service Order, subject to this Agreement. Customer may access the Service from anywhere in the world, however access to the Service from certain countries may be subject to applicable law and any technical limitations of the Service. The Service may be updated by Veritas from time to time. In order to enable Veritas to setup and/or provide the Service, Customer will provide Veritas with all necessary technical data, and other current, accurate and complete information reasonably required by Veritas for such purposes.

4. **SERVICE USAGE.**

a) **Use**. Customer will only use each Service for its internal business use, up to its applicable Registered Use Level. Customer will not resell the Service or act a service provider passing the use or benefit of the Service to third parties, unless otherwise mutually agreed through the applicable method(s) by which Veritas enrolls and permits service provider access and use, for a given Service.

b) **Lawful Use of the Service.** Customer may only use the Service for lawful business purposes. If Customer does not comply with this requirement, Veritas reserves the right to suspend all or part of the Service immediately during such non-compliance, without compensation to Customer of any kind.

c) **Changes in Service Use Level.**

1. During the Initial Period or a Renewal Period, Customer cannot reduce the Registered Use Level. The same Registered Use level will apply to the next Renewal Period, unless reduced or increased as set forth below. If Customer wishes to reduce its Registered Use Level for the next Renewal Period, Customer may do so by following Veritas’ then-current processes, as may be found in the applicable Service Description or otherwise published by Veritas.

2. At any time, Customer may purchase additional Entitlements to increase its Registered Use Level in accordance with Veritas’ then-current processes for the applicable Service.

3. If Customer’s Actual Use Level exceeds its Registered Use Level (“**Overages**”), then Veritas reserves the right to invoice for these Overages and Customer will promptly pay for such Overages. Overages fees will be at the same rates charged for the Initial Period order (or Renewal Period order), as applicable.

5. **TERM; RENEWAL.**

a) **Initial Period**. The Initial Period for a Service, which may include an initial set-up period, will begin on the date indicated in the Service Order. Customer shall ensure the information submitted at provisioning aligns with any instructions provided under this Addendum.

b) **Renewal** Subject to the End of Service Availability section below, following the Initial Period, the Service may be renewed for Renewal Periods of twelve (12) months each (unless a shorter default Renewal Period is specified in the Service Order or Service Description) upon mutual written agreement by the Parties. Customer will be responsible for submitting a timely renewal order. Any processing delays, late renewals, channel issues or other problems with the renewal order may cause the Service to expire, Service delivery to be interrupted or suspended, and, if the delay is significant, any Customer Data stored by the Service shall be deleted in accordance with the Service Description. The Service may be renewed by the Customer executing a written Order for the Renewal Period.

c) **End of Service Availability**. Veritas may notify Customer of the end-of-life (end of availability) of a given Service by giving no less than twelve (12) months prior written notice before such end of Service availability. Notwithstanding the process for other notices set forth under "General", below, Veritas may provide such notification by email to Customer's then-current business or technical contact, and/or by publication on the applicable interface(s) through which Customer's administrator interacts with the Service.

6. **TERMINATION.**

a) This Addendum, in whole or as to specific Service Order(s), may be terminated in accordance with Sections 14.2 (b) and (c) of the Agreement.

b) Upon termination of an individual Service Order, this Agreement as to all other Service Orders will continue in full force and effect. Upon termination of this Agreement in whole, all outstanding Service Orders will be terminated immediately. Termination of this Agreement will be without prejudice to any rights or liabilities accrued as of the date of termination. Veritas will be entitled to invoice and be paid for all Service(s) provided up to the effective date of termination, and all invoices become immediately then due and payable. Any term of the Agreement, which is intended to survive expiration or termination will survive, including, without limitation, confidentiality, restrictions on use of intellectual property, indemnity, limitations on liability and disclaimers of warranties and damages, governing law, and Customer's payment obligations accrued prior to termination.

7. WARRANTY. Veritas will provide the Service in a good and workmanlike manner, and substantially in accordance with the Service Description.

CUSTOMER AGREES THAT THE WARRANTIES SET FORTH IN THIS SECTION ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES OR CONDITIONS WHETHER EXPRESS OR IMPLIED CONCERNING THE SERVICE, INCLUDING, BUT NOT LIMITED TO, THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. VERITAS DOES NOT WARRANT THAT THE SERVICE WILL MEET CUSTOMER'S REQUIREMENTS OR THAT USE OF THE SERVICE(S) WILL BE UNINTERRUPTED OR ERROR-FREE.

8. INTELLECTUAL PROPERTY. The intellectual property rights in the Service are and will remain Veritas' property or that of its licensors.

9. INDEMNITY.

a) Indemnification by Veritas. (a) To the extent the Agreement includes provisions providing an express intellectual property indemnity for licensed software, such provision(s) are supplemented to add the Service(s) to the scope of the parties' obligations under such indemnification provisions, to the same extent as for such licensed software. Where Customer’s use of the Service(s) is terminated pursuant to such provisions, the Service(s) shall be returned to Veritas and Veritas' sole liability shall be to refund Customer the fees paid to Veritas for such item or portion thereof.

b) **Indemnification by Customer.** Customer agrees, at Veritas' request to defend, and to indemnify Veritas against and hold Veritas harmless from any and all claims, actions, losses, costs and expenses Veritas may incur as a result of: (i) any breach by Customer of the Section entitled "Lawful Use of the Service", (ii) Customer's unauthorized use of the Service in a manner not contemplated by the Service Description, or (iii) any third-party claim in relation to Customer Data.

10. USE AND PROTECTION OF CUSTOMER DATA AND PROVISIONING INFORMATION.

a) Veritas operates as a data processor with no control over the type, substance or format of Customer Data. Customer, as data controller, is responsible (i) to ensure that processing and disclosure of such information to Veritas complies with applicable laws; (ii) to inform users that their information will be processed by Veritas in the United States or other countries that may have less protective data protection laws than the region in which they are situated (including the European Economic Area); (iii) to inform users of how it will be used, and to assure that Customer has all appropriate consents required for such transfer and use; and (iv) to satisfy itself that the Security Standards are appropriate, given the nature of the Customer Data.

b) Veritas does not require access to or use of Customer Data to provide the Service, other than by machine-read, electronic methods and will not use or access the Customer Data unless otherwise as described in this subsection 12(b). Veritas may access or use Customer Data, if required, to enable proper functioning of the Service or as otherwise set forth in the Service Description and, in such limited circumstances, Veritas shall process Customer Data in accordance with the Customer's instructions, provided that such instructions are consistent with the terms of this Agreement. Veritas may access, use or disclose Customer Data as required by law or court order, but will give Customer prompt notice of any legally required disclosure to allow Customer to seek a protective order or other appropriate remedy (except to the extent Veritas' compliance with the foregoing would cause it to violate a court order or other legal requirement). As between Customer and Veritas, Customer Data will remain the property and Confidential Information of Customer at all times.

c) By providing the Provisioning Information, Customer acknowledges that the Provisioning Information, including any Personal Information contained within it, will be processed and accessible on a global basis by Veritas, its Affiliates agents and subcontractors for the purposes of providing the Service, to generate statistical information about the Service, for internal research and development, and as otherwise described in the Service Descriptions, including in countries that may have less protective data protection laws than in the country in which Customer or its users are located. Veritas may disclose the collected Personal Information as required or permitted by law or in response to a subpoena or other legal process. Customer also consents for itself and as agent for its contacts whose details have been provided as part of the Provisioning Information to the use by Veritas of that Personal Information for the purposes of informing Customer of Veritas products and services which may be of interest to Customer and account management. Where Customer's processing of the personal data provided to Veritas under this Agreement is subject to the General Data Protection Regulation (EU) 2016/679, or other applicable laws that relate to the processing of personal data and privacy that may exist in the European Economic Area, United Kingdom, Switzerland, Veritas shall process such personal data in accordance with the Data Processing Terms and Conditions at https://www.veritas.com/privacy. All questions and requests on privacy matters may be addressed to Veritas Technologies LLC – Privacy Program Office at Veritas' headquarters location published at veritas.com or via email: privacy@veritas.com. Veritas acknowledges that individuals may choose to opt out of direct marketing at any time on written notice to Veritas.

d) Veritas will maintain administrative, technical and physical safeguards for the Veritas Network designed to (i) protect the security and integrity of the Veritas Network, and (ii) protect against accidental or unauthorized, or unlawful access, use, alteration or disclosure of, loss, destruction or damage to, Customer

Data and Provisioning Information; and (iii) during the Term, comply with Schedule "A" (Security Requirements Schedule), as may be amended, modified, supplemented as mutually agreed in writing between the parties (the "**Security Standards**"). The "**Veritas Network**" means Veritas' data center facilities, servers, and networking equipment/software involved in hosting Customer Data and storing the Provisioning Information that are under Veritas' reasonable control and are used to provide the Service. The Security Standards will be substantially equivalent to the generally accepted security standards in the IT industry for hosted services similar to the Service. Veritas will conform to the Security Standards during the Term.

11. LIMITATION OF LIABILITY.

The Limitation of Liability provision in the Agreement is supplemented to add the following for the purposes of the Services provided under this Hosted Services Addendum, subject to all other conditions, restrictions, and disclaimers provided, therein: REGARDLESS OF THE LEGAL BASIS FOR THE CLAIM, EACH PARTY'S MAXIMUM LIABILITY UNDER THIS HOSTED SERVICES ADDENDUM WILL BE LIMITED TO THE FEES PAID OR PAYABLE BY CUSTOMER IN THE PRECEDING TWELVE (12) MONTH PERIOD FOR THE SERVICE GIVING RISE TO THE LIABILITY.

12. GENERAL. Veritas has the right to subcontract the performance of the Service to third parties, provided that Veritas remains responsible for the contractual obligations according to the Agreement and any Service Order. The terms of the Service Order, the Service Description, the Veritas Hosted Services Schedule and the Agreement shall govern, in that order of precedence, in the event of any conflict by or among such documents.

13. Miscellaneous. Capitalized terms used in this Addendum have the meanings given, and plural and possessive terms will be interpreted accordingly. In the event of a conflict between the Agreement and the terms of this Addendum, the terms of this Addendum shall prevail.

VERITAS™

MASTER LICENSE AGREEMENT

<table>
<tr><td><b>Customer Company Name:</b></td><td colspan="9"><b>General Services Administration</b></td></tr>
<tr><td><b>Address:</b></td><td colspan="9">Contact Name:
Address:

Country:

Email:

<i>(All fields are required)</i></td></tr>
<tr><td><b>Veritas Agreement Number:</b>
<i>(To be filled in by Veritas)</i></td><td></td><td></td><td></td><td></td><td></td><td></td><td>O</td><td>T</td><td>H</td></tr>
<tr><td><b>Effective Date:</b> <i>(To be filled in by Veritas upon signature)</i></td><td colspan="9"></td></tr>
</table>

This Master License Agreement ("Agreement") is entered into by and between **Veritas Technologies LLC,** a Delaware corporation**,** and Customer (identified above) as of the Effective Date defined above. This Agreement consists of these terms and conditions ("Master Terms") and any Addenda executed under these Master Terms. This Agreement applies to the Veritas software products available for purchase through the applicable GSA Schedule 70 contract from an authorized Veritas reseller, and any mention in the Agreement of "Professional Services" or other services available for additional fees does not add such services to the reseller's GSA Schedule contract.

Customer and Veritas agree as follows:

1 Definitions. All capitalized terms may be used in the singular or in the plural, as the context requires.

1.1 "Addendum" to this Agreement means any addendum, including its exhibits or attachments, executed between the parties from time to time, which references this Agreement and supplements or modifies these Master Terms.

1.2 "Business Critical Services" means Veritas's commercially-available Business Critical Services offerings, subject to the additional terms and conditions of the Business Critical Services Addenda in Attachment 4.

1.3 "Certificate" means the machine-generated certificate sent to Customer by Veritas to confirm a purchase of the applicable Licensed Software and/or Maintenance/Support and/or (at Veritas's discretion) certain Services.

1.4 "Customer" means the end user licensee named below.

1.5 "Documentation" means the user manuals and release notes accompanying the Licensed Software.

1.6 "Effective Date" of this Agreement means the relevant date assigned by Veritas upon acceptance of this Agreement.

1.7 "EULA" means Veritas's end user license agreement accompanying the Licensed Software. The only portion of the EULA that shall apply to the Licensed Software is the Section 17 (Additional Terms and Conditions) of each EULA. Such EULAs may be reviewed at any time at http://www.veritas.com/legal/eulas. For the avoidance of doubt, if an Ordering Activity places its order for Licensed Software, then such Ordering Activity is deemed to have reviewed and approved Section 17 of the applicable EULA.

1. 8 "Licensed Software" means the Veritas software products in object code form, that are commercially available on Veritas's applicable in-country price list in effect at the time of Customer's order, and any software updates provided under Maintenance/Support.

1.9 "Maintenance/Support" means the commercially-available Veritas maintenance/technical support services ordered by Customer for the Licensed Software, provided pursuant to Veritas's then-current maintenance/support policies and processes.

1.10 "Managed Security Services" means Veritas's commercially-available managed security services offerings, subject to the additional terms and conditions of the Managed Security Addenda in Attachment 5.

1.11 "MSRP" means Veritas's then-current in-country suggested list price in effect at the time of Customer's order.

1.12 "Ordering Activity" means a government entity authorized to purchase under the applicable General Services Administration federal supply schedule at the time an order is placed.

1.13 "Professional Services" means Veritas's commercially-available professional services offerings, subject to the additional terms and conditions of the Professional Services Terms Addendum in Attachment 2.

1.14 "Services" means collectively, Professional Services, Business Critical Services and Managed Security Services.

1.15 "Subscription Software" means Licensed Software licensed on a non-perpetual (term-limited) basis, as set forth in the applicable Addendum or Certificate.

1. 16 "Veritas" means the licensor entity named above.

1. 17 "Territory" means the geographic area in which Customer is authorized to purchase, install and use the Licensed Software. For purposes of this Agreement, Customer's Territory is: the United States or any U.S. Government installation sites world-wide.

1.18 "Use Level" means the license unit of measurement or model, including operating system or machine tier limitation, if applicable, by which Veritas measures, prices and sells the right to use a given Licensed Software product, in effect at the time an order is placed, as indicated in the applicable Addendum, Certificate or EULA, in that order of precedence.

2. License Grant.

2.1 Except with respect to the limited assignability of Licensed Software as set forth in Section 2.2 below, and notwithstanding any license rights to the contrary in Section 8, Utilization Limitations of the applicable GSA Schedule Contract, Veritas grants Customer, a non-exclusive, non-transferable license in the Territory to use (and to allow Customer's Ordering Activities to use) the Licensed Software in accordance with the Documentation, solely in support of Customer's and Ordering Activities internal business operations, in the quantities and at the Use Levels purchased from Veritas. The term of each Licensed Software license granted under this Agreement shall be perpetual, except for Subscription Software, for which Customer purchases a term-limited license as set forth in an applicable Addendum or Certificate. For archival purposes, Customer may make a single uninstalled copy of the Licensed Software and Documentation. All copies made pursuant to this section shall be complete copies, and shall include all copyright, trademark, and other notices in the original. Customer may not otherwise copy the Licensed Software or Documentation without Veritas's prior written consent.

Customer or Ordering Activities may allow consultant(s) or outsourcer(s) to use Customer's Licensed Software licenses to deliver dedicated services to Customer or to an Ordering Activity , so long as such use is consistent with Customer's own permitted scope of use, and is compliant with the terms of this Agreement. Customer and Ordering Activity agree that each is responsible for such third party access and use of the Licensed Software, to the same extent as if such consultant(s), outsourcer(s) or were Customer's employees.

If Customer purchases a Licensed Software license designated by Veritas for home use ("Home Use"), where available, then Customer may allow Customer's or an Ordering Activity's employee or dedicated consultant to use one copy of such Licensed Software on his or her personal home computer, provided such equipment is not owned or provided by Customer or an Ordering Activity, and provided such individual also has a computer licensed for such product at Customer's or the Ordering Activity's offices, but only for so long as such individual remains Customer's or the Ordering Activity's employee or dedicated consultant. The number of Home Use copies made and used cannot exceed the number of Home Use licenses purchased.

Veritas retains all title, copyright and other proprietary rights in the Licensed Software and Documentation, and in all copies, improvements, enhancements, modifications and derivative works thereof, including without limitation all patent, copyright, trade secret and trademark rights. Customer's rights to use the Licensed Software and Documentation shall be limited to those expressly granted in this Agreement and the applicable Addendum. All rights not expressly granted to Customer are retained by Veritas.

Non-Software Products. For any non-software products purchased by Customer under this Agreement, the terms and conditions for such products shall be as set forth in the applicable Certificates. For the avoidance of doubt, if an Ordering Activity places its order for non- software products, then such Ordering Activity is deemed to have reviewed and approved the applicable Certificate. The Dell Hardware/Appliance EULA is attached hereto as Attachment 3.

2.2 Customer may, based on its prime contract with a specific U.S. Government agency, assign Licensed Software licenses to such U. S. Government agency during the term of this Agreement. Customer must complete a License Assignment Request form in the form required by Veritas and otherwise comply with Veritas's then-current License Assignment Policy. Such assignment shall be at no additional cost to the U.S. Government, except for subsequent renewal of Maintenance/Support services, which the subject U.S. Government agency may or may not elect to procure. If Customer has obtained Maintenance/Support services in support of the Licensed Software, then Customer shall assign the remainder of any associated Maintenance/Support services to the U.S. Government agency to which Customer assigns the Licensed Software. Any U.S. Government agency to which Customer assigns Licensed Software and Maintenance/Support services under this Section must agree in writing to be bound by the terms and conditions of this Agreement. Certain purchasing Addenda may limit Customer's right to assign licenses purchased under and during the term of such Addenda.

3. License Restrictions. Customer shall not, without Veritas's prior written consent, conduct, cause or permit the: (a) use, copying, modification, rental, lease, sublease, sublicense, or transfer of the Licensed Software or Documentation, except as expressly provided in this Agreement; (b) creation of any derivative works based on the Licensed Software or Documentation; (c) reverse engineering, disassembly, or decompiling of the Licensed Software (except that Customer may decompile the Licensed Software for the purposes of interoperability only to the extent permitted by and subject to strict compliance under applicable law); (d) use of the Licensed Software or Documentation in connection with a service bureau or like activity whereby Customer, without purchasing a service bureau license from Veritas, operates or uses the Licensed Software or Documentation for the benefit of a third party; or (e) use of the Licensed Software or Documentation by any party other than Customer. In addition, Customer shall only use the number and type of Licensed Software licenses for which it has purchased an appropriate quantity and Use Level.

4. Orders. Customer may acquire copies of the Licensed Software, Maintenance/Support, Professional Services, Business Critical Services and/or Managed Security Services by submitting a Purchase Order to Veritas or to a Veritas Authorized Reseller.

5. Delivery.

5.1 **Delivery – Direct Orders to Veritas**. Customer elects to receive all Licensed Software via electronic download where available, and via tangible format where electronic download is not available. Customer acknowledges that Veritas may deliver upgrades and patches to Licensed Software under Maintenance/Support using tangible media as part of mass mailings. The terms of any physical delivery shall be F.O.B. destination.

5.2 **Delivery – Orders to Veritas Authorized Reseller**, Veritas shall not be responsible for delivery under terms other than those stated in Section 5.1, notwithstanding that Customer and a Veritas Authorized Reseller may negotiate other delivery terms.

6. Maintenance/Support. Customer may purchase Maintenance/Support for the applicable Licensed Software. Maintenance/Support is provided and performed subject to Veritas's then-current policies and processes. Veritas may amend its Enterprise Technical Support Policy from time to time in its sole discretion; provided, however, that for a period of five (5) years from the Effective Date of this Agreement, Veritas agrees that any such changes shall not significantly degrade the material elements of the Maintenance/Support plan offering provided to Customer. Substantive revisions of such Maintenance/Support policies or processes shall apply to Customer only when Maintenance/Support is renewed. Current Maintenance/Support terms and conditions are available at http://go.veritas.com/support- fundamentals.

7. Services.
(a) **Professional Services**. Customer may purchase Services, which are provided and performed pursuant to the Professional Services Terms Addendum in Attachment 1 and any applicable statement(s) of work.

(b) **Business Critical Services**. Customer may purchase such Business Critical Services, which are provided and performed pursuant to Attachment 3.

(c) Managed Security Services. Customer may purchase such Managed Security Services, which are provided and performed pursuant to Attachment 4.

8. Payment Terms; Taxes
8.1 **Payment.**
8.1.1 **Payment Terms – Direct Orders to Veritas**. Customer shall pay all invoices according to the terms of the applicable GSA Schedule Contract.

8.1.2 **Payment Terms – Orders to Veritas Authorized Reseller**. For orders placed with a Veritas Authorized Reseller, payment shall be in accordance with the terms and conditions negotiated between the Veritas Authorized Reseller and the Customer.

8.2 **Taxes**.
Taxes will not apply to charges for products or services directly paid for by the Federal Government, if such exemption is allowed by the tax jurisdiction in which the products or services are delivered.

9. Warranties.
9.1 Media. If Veritas provides Customer tangible media for Licensed Software, Veritas warrants that the magnetic media upon which the Licensed Software is recorded will not be defective under normal use, for a period of ninety (90) days from delivery. Veritas will replace any

defective media returned to it within the warranty period at no charge to Customer.

9.2 Licensed Software**.** Veritas warrants that the Licensed Software, as delivered by Veritas and when used in accordance with the Documentation, will substantially conform to the Documentation for a period of ninety (90) days from delivery. If the Licensed Software does not comply with this warranty and such non-compliance is reported by Customer to Veritas within the ninety (90) day warranty period, Veritas will do one of the following, selected at Veritas's reasonable discretion: either (a) repair the Licensed Software, (b) replace the Licensed Software with software of substantially the same functionality, (c) terminate the license and refund the relevant license fees paid for such non-compliant Licensed Software, or (d) in the case of software updates provided under Maintenance/Support, refund the relevant Maintenance/Support fees. The above warranties specifically exclude defects resulting from accident, abuse, unauthorized repair, modifications or enhancements, or misapplication.

9.3 Maintenance/Support and Business Critical Services**.** Veritas warrants, for a period of thirty (30) days from the date of performance of Maintenance/Support, that such Maintenance/Support will be performed in a manner consistent with generally accepted industry standards. For Maintenance/Support not performed as warranted in this provision, and provided Customer has reported such non-conformance to Veritas within thirty (30) days of performance of such non-conforming Maintenance/Support, Veritas will, in its reasonable discretion either correct any nonconforming Maintenance/Support or refund the relevant fees paid for the nonconforming Maintenance/Support.

9.4 Professional Services and Managed Security Services.

(a) Professional Services. Veritas will provide the Professional Services described in the Statement of Work ("SOW") in a good and workmanlike manner and in accordance with generally accepted industry standards.

(b) Managed Security Services. Unless otherwise specified in the Managed Security Services Certificates attached hereto, the Managed Security Service(s) will be performed in a good and workmanlike manner and in accordance with: (a) generally accepted industry standards; and (b) the service level warranties indicated in the applicable Managed Security Service(s) Certificates.

9.5 Disclaimer of Warranties; Exclusive Remedies. THE WARRANTIES SET FORTH IN THIS SECTION 9 ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, CONCERNING THE LICENSED SOFTWARE AND RELATED MAINTENANCE/SUPPORT. THE REMEDIES SET FORTH ABOVE IN THIS SECTION 9 ARE CUSTOMER'S EXCLUSIVE REMEDY AND VERITAS'S SOLE LIABILITY WITH RESPECT TO THE APPLICABLE EXPRESS WARRANTIES SET FORTH ABOVE. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW VERITAS EXPRESSLY DISCLAIMS ALL OTHER WARRANTIES, INCLUDING ANY IMPLIED WARRANTIES OF SATISFACTORY QUALITY, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND STATUTORY OR OTHER WARRANTIES OF NON-INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS WITH RESPECT TO THIS AGREEMENT AND ITEMS OR ACTIVITIES CONTEMPLATED HEREUNDER. VERITAS DOES NOT WARRANT THAT THE LICENSED SOFTWARE SHALL MEET CUSTOMER'S REQUIREMENTS OR THAT USE OF THE LICENSED SOFTWARE SHALL BE UNINTERRUPTED OR ERROR FREE.

10. Intellectual Property Claims.

10.1 Veritas shall defend, indemnify and hold Customer harmless from any claim asserting that the Licensed Software infringes any intellectual property right of a third party, and shall pay any and all damages finally awarded against the Customer by a court of final appeal, or agreed to in settlement by Veritas and attributable to such claim. Veritas's obligations under this provision are subject to Customer's doing the following: notifying Veritas of the claim in writing, as soon as Customer learns of it; providing Veritas all reasonable assistance and information to enable Veritas to perform its duties under this Section. Notwithstanding the foregoing, Customer, through the Attorney General, acting by and through the attorneys of the US Department of Justice, may participate at Customer's expense in the defense of any such claim. Customer has the right to approve any settlement that affirmatively places on Customer an obligation that has a material adverse effect on Customer other than the obligations to cease using the affected Licensed Software or to pay sums indemnified hereunder. Such approval will not be unreasonably withheld.

10.2 If the Licensed Software is found to infringe, or if Veritas determines in its sole opinion that it is likely to be found to infringe, then Veritas shall either (a) obtain for Customer the right to continue to use the Licensed Software; or (b) modify the Licensed Software so as to make such Licensed Software non-infringing, or replace it with a non-infringing equivalent substantially comparable in functionality in which case Customer shall stop using any infringing version of the Licensed Software, or (if Veritas determines in its sole opinion that (a) and/or (b) are not commercially reasonable), (c) terminate Customer's rights and Veritas**'s** obligations under this Agreement with respect to such Licensed Software, and refund to Customer the license fee paid for the relevant Licensed Software, and provide a pro-rated refund of any unused, prepaid Maintenance/Support fees paid by Customer for the applicable Licensed Software.

10.3 Notwithstanding the above, Veritas will have no liability for any infringement claim to the extent that it is based upon: (a) modification of the Software other than by Veritas; (b) combination, use, or operation of the Licensed Software with products not specifically authorized by Veritas to be combined with the Software as indicated in the Documentation; (c) use of the Licensed Software other than in accordance with the Documentation and this Agreement; or (d) Customer's continued use of infringing Licensed Software after Veritas, for no additional charge, supplies or offers to supply modified or replacement non-infringing Licensed Software as contemplated under 10.2(b) above.

THIS SECTION 10 STATES CUSTOMER'S SOLE AND EXCLUSIVE REMEDY AND VERITAS'S SOLE AND EXCLUSIVE LIABILITY REGARDING INFRINGEMENT OR MISAPPROPRIATION OF ANY INTELLECTUAL PROPERTY RIGHTS OF A THIRD PARTY.

11. LIMITATION OF LIABILITY. EXCEPT AS LIMITED BY APPLICABLE LAW, THE FOLLOWING SHALL APPLY NOTWITHSTANDING THE FAILURE OF THE ESSENTIAL PURPOSE OF ANY LIMITED REMEDY AND REGARDLESS OF THE LEGAL BASIS FOR A CLAIM: IN NO EVENT SHALL EITHER PARTY BE LIABLE TO THE OTHER PARTY OR TO ANY PERSON FOR (i) ANY COSTS OF PROCUREMENT OF SUBSTITUTE OR REPLACEMENT GOODS AND SERVICES, LOSS OF PROFITS, LOSS OF USE, LOSS OF OR CORRUPTION TO DATA, BUSINESS INTERRUPTION, LOSS OF PRODUCTION, LOSS OF REVENUES, LOSS OF CONTRACTS, LOSS OF GOODWILL, OR ANTICIPATED SAVINGS OR WASTED MANAGEMENT AND STAFF TIME; OR (ii) ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL OR INDIRECT DAMAGES WHETHER ARISING DIRECTLY OR INDIRECTLY OUT OF THIS AGREEMENT.

THE FOREGOING SHALL APPLY EVEN IF (SUCH PARTY, ITS RESELLERS, SUPPLIERS OR ITS AGENTS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. EXCEPT FOR LIABILTY ARISING FROM VERITAS'S OBLIGATIONS UNDER SECTION 10 (INTELLECTUAL PROPERTY CLAIMS), OR LIABILITY ARISING FROM BREACH OF SECTION 12 (CONFIDENTIALITY) OR FROM CUSTOMER'S BREACH OF ITS PERMITTED SCOPE OF AUTHORIZED USE UNDER THIS AGREEMENT, AND REGARDLESS OF THE LEGAL BASIS FOR THE CLAIM, EACH PARTY'S MAXIMUM LIABILITY UNDER THIS AGREEMENT SHALL NOT EXCEED THE FEES PAID OR OWED FOR THE LICENSED SOFTWARE, MAINTENANCE/SUPPORT SERVICES OR HARDWARE GIVING RISE TO THE CLAIM. NOTHING IN THIS AGREEMENT SHALL EXCLUDE

OR LIMIT A PARTY'S LIABILITY FOR ANY LIABILITY WHICH CANNOT BE EXCLUDED OR LIMITED BY LAW. This Section 11, "Limitation of Liability", shall not impair the U.S. Government's right to recover for fraud or crimes arising out of or related to this Contract under any federal fraud statute, including the False Claims Act, 31 U.S.C. §§ 3729-3733. Furthermore, this clause shall not impair nor prejudice the U.S. Government's right to EXPRESS remedies provided in the applicable Schedule Contract (i.e. clause 552.238-72 – Price Reductions, clause 52.212-4(h) – Patent Indemnification, Liability for Injury or Damage (Section 3 of the Price List), and GSAR 552.215-72 – Price Adjustment – Failure to Provide Accurate Information).

12. Confidentiality.

12.1 "Confidential Information" means the non-public information that is exchanged between the parties, provided that such information is:
(a) identified as confidential at the time of disclosure by the disclosing party ("Discloser"), or (b) disclosed under circumstances that would indicate to a reasonable person that the information ought to be treated as confidential by the party receiving such information ("Recipient"). A Recipient may use the Confidential Information that it receives from the other party solely for the purpose of performing activities contemplated under this Agreement ("Purpose"). For a period of five (5) years following the applicable date of disclosure of any Confidential Information, a Recipient shall hold the Confidential Information in confidence and not disclose the Confidential Information to any third party. A Recipient shall protect the Confidential Information by using the same degree of care, but no less than a reasonable degree of care, to prevent the unauthorized use, dissemination or publication of the Confidential Information as the Recipient uses to protect its own confidential information of a like nature. The Recipient may disclose the Confidential Information to agents and independent contractors with a need to know in order to fulfill the Purpose who have signed a nondisclosure agreement at least as protective of the Discloser's rights as this Agreement.

12.2 This provision imposes no obligation upon a Recipient with respect to Confidential Information which: (a) is or becomes public knowledge through no fault of the Recipient; (b) was in the Recipient's possession before receipt from the Discloser and was not subject to a duty of confidentiality; (c) is rightfully received by the Recipient without any duty of confidentiality; (d) is disclosed generally to a third party by the Discloser without a duty of confidentiality on the third party; or (e) is independently developed by the Recipient without use of the Confidential Information. The Recipient may disclose the Discloser's Confidential Information as required by law or court order provided: (i) the Recipient promptly notifies the Discloser in writing of the requirement for disclosure; and (ii) discloses only as much of the Confidential Information as is required. The Recipient's obligations with respect to the Confidential Information hereunder will survive any termination of the Agreement. Upon request from the Discloser or upon termination of the Agreement the Recipient shall return to the Discloser all Confidential Information and all copies, notes, summaries or extracts thereof or certify destruction of the same, except information that qualifies as a "Government Record" under the Federal Records Act (44 USC 3301).

12.3 Each party will retain all right, title and interest to such party's Confidential Information. Neither party to this Agreement acquires any patent, copyright or other intellectual property rights or any other rights or licenses under this Agreement except the limited right to use for fulfillment of the Purpose, as set forth in section 12.1 above. Nothing in this provision shall be construed to preclude either party from developing, using, marketing, licensing, and/or selling any product or service that is developed without use of the Confidential Information.

13. Verification. Except where prohibited by applicable federal law or security regulations, Customer or Ordering Activity as appropriate, agrees to keep accurate business records relating to its use and deployment of the Licensed Software. Upon thirty (30) days prior written notice, Customer agrees to provide Veritas written reports related to Customer's use of the Licensed Software to verify Customer's compliance with its obligations under this Agreement. Such report shall include, at a minimum, the product name (including any options, agents and extensions), version number, quantity of each product, and the operating system/platform, hardware model, Host ID and street address location of the Designated Computer on each such copy is installed. In the event that Customer fails to provide reports acceptable to Veritas; once annually, Veritas may verify Customer's compliance with this Agreement by reviewing (upon five (5) business days' prior written notice) Customer's use and deployment of the Licensed Software. Either Veritas or an independent public accounting firm reasonably acceptable to both parties shall perform the audit during Customer's regular business hours with minimal disruption to Customer's ongoing business operations and adherence to any security measures the Customer deems appropriate, including any requirements under Federal security regulations that may require personnel clearances prior to accessing sensitive information or facilities. Any nondisclosure agreement Customer may require the independent public accounting firm to execute shall not prevent disclosure of the audit results to Veritas. All audits shall be subject to Customer's reasonable safety and security policies and procedures. In the event unauthorized deployments of Veritas products are disclosed by the audit, Veritas will submit a claim to the contracting officer of the Customer or relevant Ordering Activity.

14. Term and Termination.

14.1 Term**.** Unless terminated as set forth in the applicable GSA Schedule Contract, these Master Terms shall continue indefinitely, and each Addendum shall continue for the term set forth in such Addendum.

14.2 Termination**.**
The provisions of this Agreement regarding confidentiality, restrictions on use of intellectual property, limitations on liability and disclaimers of warranties and damages, audit, and Customer's payment obligations accrued prior to termination, shall survive any termination. The license grants for Licensed Software and terms regarding Maintenance/Support purchased prior to termination shall survive such termination.

15. General

15.1 Governing Law; Severability; Waiver. This Agreement shall be governed by and construed in accordance with the laws of the United States. Such application of law excludes any provisions of the United Nations Convention on Contracts for the International Sale of Goods, including any amendments thereto, and without regard to principles of conflicts of law. If any provision of this Agreement is found partly or wholly illegal or unenforceable, such provision shall be enforced to the maximum extent permissible, and the legality and enforceability of the other provisions of this Agreement shall remain in full force and effect. A waiver of any breach or default under this Agreement shall not constitute a waiver of any other right for subsequent breach or default.

15.2 Assignment**.** Except with respect to the Licensed Software as set forth in Section 2.2 above, and subject to FAR 42.12 (Novation and Change of Name Agreements and its successor regulations), neither party may assign this Agreement, in whole or in part and whether by operation of contract, law or otherwise, without the other party's prior written consent. Such consent shall not be unreasonably withheld or delayed. For purposes of this provision, a change of control shall constitute an assignment. Notwithstanding the foregoing, either party may, upon written notice to the non-assigning party, (i) assign this Agreement to a successor in interest to all or substantially all of its assets, whether by sale, merger, or otherwise, (ii) assign this Agreement to a parent company; or (iii) assign this Agreement to a wholly-owned subsidiary. All terms and conditions of the Agreement shall be binding upon any assignee hereunder; assignee's acceptance of these terms shall be evidenced by its performance hereunder.

15.3 Export. Customer acknowledges that the Licensed Software and related technical data and services (collectively "Controlled Technology") may be subject to the import and export laws of the United

States, specifically the U.S. Export Administration Regulations (EAR), and the laws of any country where Controlled Technology is imported or re-exported. Customer agrees to comply with all relevant laws and will not to export or re-export any Controlled Technology in contravention to U.S. law, nor to any prohibited country, entity, or person for which an export license or other governmental approval is required. All Controlled Technology is prohibited for export or re-export to Cuba, North Korea, Iran, Syria and Sudan and to any country subject to relevant trade sanctions. Customer hereby agrees that it will not export, re-export or sell any Controlled Technology for use in connection with chemical, biological, or nuclear weapons, or missiles, drones or space launch vehicles capable of delivering such weapons.

15.4 Government Rights. The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR Part 12 and its successor regulations, and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the Government shall be solely in accordance with the terms of this Agreement.

15.5 Entire Agreement**.** Any subsequent modifications to this Agreement shall be made in writing and must be duly signed by authorized representatives of both parties or they shall be void and of no effect. Unless an Ordering Activity and Veritas negotiate alternative terms, this Agreement prevails.

Order of precedence. Notwithstanding anything in this Agreement to the contrary, any inconsistencies in this Agreement shall be resolved by giving precedence in the following order:
(1) The schedule of supplies/services.
(2) The Assignments, Disputes, Payments, Invoice, Other Compliances, Compliance with Laws Unique to Government Contracts, Unauthorized Obligations, and Commercial Supplier Agreements – Unenforceable Clauses paragraphs of this clause,
(3) The clause at 52.212-5,
(4) Solicitation provisions if this is a solicitation.
(5) Other paragraphs of this clause.
(6) Addenda to this solicitation or contract, including any license agreements for computer software.
(7) The Standard Form 1449.
(8) Other documents, exhibits, and attachments.
(9) The specification.

15.6 Force Majeure. Each party shall be excused from performance (other than payment obligations) for any period during which, and to the extent that, it is prevented from performing any obligation or service, in whole or in part, due to unforeseen circumstances or to causes beyond such party's reasonable control, including but not limited to acts of God, war, terrorism, riot, embargoes, acts of civil or military authorities, fire, floods, accidents, strikes, regulatory requirements or shortages of transportation, facilities, fuel, energy, labor or materials.

15.7 Notices. All notices required to be sent hereunder shall be in writing addressed to the relevant Contracting Officer or to Veritas's corporate headquarters, with a simultaneous cc: to the attention of Veritas's Legal Department/General Counsel. Notices shall be effective upon receipt, and shall be deemed to have been received as follows: (a) if personally delivered by courier, when delivered; (b) if mailed by first class mail, on the fifth business day after deposit in the mail with the proper address; or (c) if by certified mail, return receipt requested, on the date received.

15.8 Signatures. Facsimile signatures and signed facsimile copies of this Agreement, its Addenda, attachments and exhibits shall legally bind the parties to the same extent as originals. This Agreement with its accompanying Addendum/Addenda may be executed in multiple counterparts all of which taken together shall constitute one single agreement between the parties. The signatories hereto represent that they are duly authorized to sign this Agreement on behalf of their respective companies.

15.9 Subcontractors. Veritas may assign the Service(s) (Maintenance/Support, Business Critical Services or Managed Security Services) or any part thereof, and may additionally subcontract the Agreement and / or Service(s), provided that it remains responsible for any subcontractors performing on its behalf.

Attachment 1 – Professional Services Addendum

Attachment 2 – Hardware Warranty Agreement (Veritas 8160/8360/8380)

Attachment 3 – Business Critical Services

Attachment 4 – Managed Security Services

ATTACHMENT 1

PROFESSIONAL SERVICES TERMS ADDENDUM

VERITAS™

ATTACHMENT 1

PROFESSIONAL SERVICES TERMS ADDENDUM

1. Statements of Work (a) During the Term (as defined in Section 2 below) Veritas and Customer (including Ordering Activity) may agree upon a written statement of work, quote/order form, or certificate under this Addendum (**"SOW"**), that may include descriptions of services to be performed by Veritas ("**Professional Services**") and deliverables **("Deliverables")** to be provided by Veritas, fees, duration and renewal of the Professional Services, and other responsibilities undertaken by Customer and/or Veritas. Certain Professional Services may require software, hardware and associated documentation to be separately provided by Veritas as part of the Service ("**Service Components**"). This Addendum will control in the event of any conflict with a SOW, unless otherwise specified in the SOW. However, the SOW may contain terms and conditions specific to the applicable Professional Services ordered which terms will have no effect on other SOWs.

2. Term; Termination. "**Term**" means the applicable effective period of this Addendum and/or of Professional Services under a Purchase Order or SOW. The Term of this Addendum will begin on the Effective Date and continue until termination. The Term for any Professional Services provided under this Addendum, which may include an initial set-up period, will be as set forth in the applicable Purchase Order or SOW and may be extended by mutual agreement of the parties. . This Addendum and/or a SOW may be terminated in accordance with the terms of the applicable GSA Schedule contract.

3. The Purchase Order issued by the Ordering Activity shall include any additional terms and conditions negotiated between Veritas and the Ordering Activity regarding payment for Professional Services fees, travel and living expenses incurred in the course of performance and reseller fees.

4. Rights in Deliverables.

(a) Ownership Rights. Subject to Veritas's rights in Veritas Information and Veritas Derivative Work as each are defined below, all Deliverables created specifically for and provided to Customer by Veritas under an SOW will, upon final payment, become the property of Customer for Customer's internal business purposes. Any inventions, designs, intellectual property or other derivative works of Veritas Information, will vest in and be the exclusive property of Veritas ("**Veritas Derivative Work**"). Any inventions, designs, intellectual property or other derivative works of Customer Information (as defined below) will vest in and be the exclusive property of Customer ("**Customer Derivative Work**").

(b) Pre-Existing Work. Any pre-existing proprietary or Confidential Information of Veritas or its licensors used to perform the Professional Services, or included in any Deliverable, including, but not limited to Service Components, software, appliances, methodologies, code, templates, tools, policies, records, working papers, know-how, data or other intellectual property, written or otherwise, including Derivative Works will remain the exclusive property of Veritas and its licensors (collectively, "**Veritas Information**"). Any Customer pre-existing information, including but not limited to any Customer proprietary and Confidential Information provided to Veritas by Customer will remain the exclusive property of Customer or its licensors ("**Customer Information**"). For the purposes of this Addendum, Veritas Information and Customer Information will be deemed Confidential Information.

(c) Retention. Customer acknowledges that Veritas provides similar services to other customers and that nothing in this Addendum or a SOW will be construed to prevent Veritas from carrying on such business. Customer acknowledges that Veritas may at its sole discretion develop, use, market, distribute and license substantially similar Deliverables. Notwithstanding the preceding sentence, Veritas agrees that it will not market or distribute any Deliverables that include the Confidential Information of Customer.

(d) License Grant. In consideration of Customer's payment of applicable Fees, Veritas grants Customer a limited, non-exclusive, non-transferable license, to access and use, in accordance with the SOW and solely for Customer's internal business purposes: (i) Veritas Information, to the extent such information is necessary to utilize the Professional Services or incorporated into any Deliverable; and (ii) Service Components in the format provided by Veritas, for use on systems under Customer's control, solely in connection with the Professional Services for which such Service Components are provided.

(e) License Restrictions. Customer will not act to infringe the intellectual property rights of Veritas or its licensors, including Veritas Information. Other than as expressly permitted under this Addendum or applicable law, Customer will not copy, sublicense, sell, rent, lease or otherwise distribute Veritas Information, or permit either direct or indirect use of Veritas Information by any third party. Customer will not modify, reverse engineer, disassemble, decompile, or create derivative works of Veritas Information, or otherwise attempt to build a competitive product or service using Veritas Information. Notwithstanding the foregoing, the license grant set forth above may be further limited as set forth in any applicable SOW.

(f) In the event that Customer, based on its prime contract with the U.S. Government, requires that data from analysis tasks performed under a SOW be transferable to a specific U.S. Government agency, then Customer shall identify the prime contract number and the U.S. Government Agency in that SOW. Veritas will allow the transfer request to the specified U.S. Government Agency under the prime contract number identified in the SOW. The rights in technical data transferred to the U.S. Government under the prime contract number identified in a SOW are set forth in Section (g) below. This provision will only apply to an Ordering Activity if the parties so state in an applicable SOW with such Ordering Activity.

(g) Government Rights. The data resulting from analysis tasks performed under an applicable SOW are deemed to be Commercial Items as defined in FAR Part 12 and its successor regulations, subject to restricted rights as defined in DFARS 252.227-7015, "Technical Data – Commercial Items", and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of such data by the U.S. Government agency identified in the applicable SOW shall be solely in accordance with the terms of this Agreement.

5. Intellectual Property Indemnification.

a) To the extent the Addendum includes provisions providing an express intellectual property indemnity for Licensed Software, such provision(s) are supplemented to add the Deliverables to the scope of the parties' obligations under such indemnification provisions, to the same extent as for such Licensed Software. Where Customer's use of the Deliverables is terminated pursuant to such provisions, the Deliverables shall be returned to Veritas and Veritas's sole liability, in addition to its indemnification obligations herein, shall be to refund to Customer the fees paid to Veritas for the relevant Services or portion thereof.

b) In the event that any willful misconduct or grossly negligent act or omission of a Party or its employees during the performance of Professional Services on Customer's premises causes or results in the (i) loss, damage to or destruction of physical property of the other Party or third parties, and/or (ii) death or injury to any person, then such Party will indemnify, defend and hold the Party harmless from and against any and all resulting claims, damages, liabilities, costs and expenses (including reasonable attorney's fees), subject to the Limitation of Liability of the Master Agreement, as supplemented below.

6. Non-Solicitation. During the Term of any applicable SOW, and for a period of one (1) year thereafter, neither Party will actively solicit for hire, nor knowingly allow its employees to solicit for hire, any employee of either Party associated with the performance of Professional Services under the applicable SOW without the prior written consent of the other Party. This provision will in no way restrict the right of either Party to solicit generally in the media for required personnel, and will not restrict employees, contractors, or representatives of either Party from pursuing on their own initiative employment opportunities from or with the other Party. In the event a Party violates this provision, the Parties may mutually agree to liquidated damages.

7. Data Privacy. For the purpose of providing Professional Services pursuant to this Addendum, Veritas will require Customer to supply certain personal information e.g. business contact names, business telephone numbers, business e-mail addresses. Customer acknowledges that Veritas is a global organization, and such personal information may be accessible on a global basis by Veritas affiliates or Veritas partners and subcontractors, including in countries that may have less protective data protection laws than the country in which Customer is located. By providing such personal information, Customer consents to Veritas using, transferring and processing this information on a global basis for the use described above. For any question regarding the use of personal information, Customer may contact Veritas Technologies LLC - Privacy Lead, 500 East Middlefield Road, Mountain View, CA 94043, U.S.A. Telephone (650) 933-1000 Email: privacy@veritas.com.

8. Miscellaneous. (a) While on Customer's premises, Veritas will ensure that its personnel follow all reasonable instructions, as such are provided to Veritas prior to the performance of the Professional Services. **(b)** Veritas is an independent contractor and will not be deemed an employee or agent of Customer. **(c)** Veritas has the right to subcontract the performance of the Professional Services to third parties, provided that Veritas remains responsible for the contractual obligations according to this Addendum and any SOW.

VERITAS™

Attachment 2
Hardware Appliance Warranty

Attachment 2
Hardware Appliance Warranty

1. **HARDWARE/SOFTWARE.** The hardware ("Hardware") that accompanies this Warranty Agreement is to be used only with the Licensed Software. "Licensed Software" means the Veritas software product, in object code form, that is pre-loaded, pre-installed, or included as a media kit accompanying the Hardware, including any documentation provided with such software. You may not use the Licensed Software unless You have purchased a separate license for such Licensed Software. Your use of the Licensed Software shall comply with the terms and conditions of the Master License Agreement that has been accepted as part of the applicable GSA Schedule contract and the License Instrument applicable for such Licensed Software. "License Instrument" means one or more of the following applicable documents which further defines Your license rights to the Licensed Software: a Veritas license certificate or a similar license document issued by Veritas, or a written agreement between You and Veritas, that accompanies, precedes or follows the Master License Agreement for the Licensed Software.

2. **OWNERSHIP.** The Licensed Software is the proprietary property of Veritas or its licensors and is protected by copyright law. Veritas and its licensors retain any and all rights, title and interest in and to the Licensed Software, including in all copies, improvements, enhancements, modifications and derivative works of the Licensed Software. Your rights to use the Licensed Software shall be limited to those expressly granted in this Warranty Agreement. All rights not expressly granted to You are retained by Veritas and/or its licensors.

3. **GEOGRAPHIC USE LOCATION.** Prior to using the Hardware, You must register a service tag for such Hardware in the location You intend to use the Hardware ("Geographic Use Location"). In the event You wish to change Your Geographic Use Location, You must re-register the Hardware using the tag transfer process located at https://www.veritas.com/support/en_US/contact. Any change to the Geographic Use Location and/or any service request which requires Veritas to obtain additional information and/or validate information to acknowledge and approve warranty service entitlements may result in a delay in providing such warranty service entitlements.

4. **LIMITED WARRANTY.** Veritas warrants that the Hardware shall be free from defects in material and workmanship under normal authorized use and service and will substantially conform to the written documentation accompanying the Hardware for the applicable Warranty Period (defined in this Section 4) and as specified at the time of original purchase and in the packing slip documentation accompanying Your Hardware. The standard warranty period is three (3) years from the date of original purchase of the Hardware ("Standard Warranty Period"). However, if at time of original purchase You acquired extended warranty, as indicated in the packing slip documentation accompanying Your Hardware, the Hardware shall be warranted for a period of up to five (5) years from the date of original purchase ("Extended Warranty Period"). "Standard Warranty Period" and "Extended Warranty Period" shall collectively be referred to as "Warranty Period". Upon confirmation of a defect or failure of a Hardware, or component thereof, to perform as warranted in this Section 4, and depending on the then-current Geographic Use Location of the Hardware, Your sole and exclusive remedy for defective Hardware, or component thereof, if notified within the Warranty Period, shall be for Veritas, at its sole option and discretion, to:

(i) repair or replace the defective Hardware, or component thereof, with either a new or refurbished replacement Hardware, or component thereof, as applicable;

(ii) provide onsite repair services for any defective Hardware, or component thereof; or

(iii) repair or replace any defective Hardware returned to Veritas through Veritas's Returned Merchandise Authorization Services process for Hardware.

All defective Hardware, or component thereof, which has been replaced, shall become the property of Veritas. All defective Hardware, or component thereof, which has been repaired shall remain Your property. **EXCEPT FOR THE SPECIFIC WARRANTIES OR REMEDIES SET FORTH UNDER THE APPLICABLE GSA SCHEDULE, THE FOREGOING IS YOUR SOLE AND EXCLUSIVE REMEDY, AND VERITAS'S SOLE AND EXCLUSIVE LIABILITY FOR VERITAS'S BREACH OF THIS LIMTED WARRANTY.**

5. **LIMITED HARDWARE WARRANTY SUPPORT SERVICES.** During the Warranty Period, warranty support services will be provided in accordance with (i) the service procedures identified by Veritas in Section 7, below, and (ii) the then-current Veritas Enterprise Technical Support Policy in accordance with Section 6 (Maintenance/Support) of the Agreement

The Geographic Use Location of the Hardware will determine whether You are entitled to either warranty service consisting of (a) Next Business Day Service, (b) Same Day Service or (c) Return Merchandize Authorization Services as detailed below in this Section 5. Upon discovery of any failure of the Hardware, or component thereof, during the Warranty Period, the following options are available to You.

A. <u>**Next Business Day Service**</u>. You may initiate a request for next business day onsite repair services if You have purchased such services as part of Your warranty support. A service technician will, in most cases, be dispatched to arrive at Your location for onsite repair services on the next business day; Monday through Friday 8:00 AM to 6:00 PM local time, excluding regularly observed holidays. If the service technician is dispatched for onsite repair services after 5:00 PM local time, the service technician may take additional business day(s) to arrive at Your Geographic Use Location.

B. <u>**Same Day Service**</u>. If You have purchased the optional same day service upgrade, then for an additional fee and if offered in the then current Geographic Use Location, You may initiate a request for same day onsite services. A service technician will, in most cases, be dispatched to arrive at Your location for onsite service within the same day after dispatch, twenty-four (24) hours a day, seven (7) days a week (including holidays), provided the service location is between one hundred twenty-five (125) miles from the nearest parts stocking location.

C. <u>**Return Merchandise Authorization Process**</u>. In the event Veritas does not have Next Business Day Service, or Same Day Service available in Your then current Geographic Use Location or, if, Veritas determines in its sole discretion that Next Business Day**,** or Same Day Service may not be appropriate You are required to contact Veritas within ten (10) days after such failure and seek a return material authorization ("RMA") number. Veritas will promptly issue the requested RMA as long as Veritas determines that You meet the conditions for warranty service. The allegedly defective Hardware, or component thereof, shall be returned to Veritas, securely and properly packaged, freight and insurance prepaid, with the RMA number prominently displayed on the exterior of the shipment packaging and with the Hardware. Veritas will have no obligation to accept any Hardware which is returned without an RMA number. Veritas reserves the right, in its sole option, to repair or replace defective Hardware, or component thereof. With respect to a return of defective Hardware, or component thereof, Veritas and Customer or Ordering Activity will negotiate mutually agreeable transportation or other direct costs. With respect to a return of functional Hardware, or return of Hardware ordered in error by Customer, Customer will pay any transportation costs. Any credits are subject to Veritas's then-current RMA (Return Materials Authorization) policies/process.

6. **SERVICE PARTS INSTALLATION.** Regardless of the service response level purchased, some component parts are specifically designed for easy removal and replacement by You: such parts are designated as Customer Self Replaceable ("**CSR**"). If during the troubleshooting and diagnosis, the Veritas technical support analyst determines that the repair can be accomplished with a CSR designated part, Veritas will ship the CSR designated part directly to You. CSR parts fall into two categories:

(A) **Optional CSR parts.** Optional CSR parts are designed for simple installation by You; however, depending on the type of service that was purchased with the Supported Product, Veritas may provide an onsite technician to replace the parts.

(B) **Mandatory CSR parts.** Mandatory CSR parts are designed for simple installation by You and Veritas does not provide installation labor services to install Mandatory CSR parts. If You request that Veritas and/or the Veritas Authorized Reseller replace these parts, You will be charged a fee for this service.

7. **HARDWARE WARRANTY SERVICE PREQUISITES. IN ORDER TO EXERCISE ANY OF THE WARRANTY RIGHTS CONTAINED IN THIS WARRANTY AGREEMENT, YOU MUST COMPLY WITH THE FOLLOWING PROCEDURES:**

(A) have available an original sales receipt or bill of sale demonstrating proof of purchase with Your warranty claim;

(B) separately procure and maintain during the entire Warranty Period, an active maintenance contract for the Licensed Software, as designated by Veritas and corresponding support ("Software Support and Maintenance");

(C) identify for Veritas the then current Geographic Use Location for the Hardware, in accordance with Veritas's requirements.

(D) Prepare for the Call. You must have the following information and materials ready when You call the technician: Your system's invoice and serial numbers; the then current Geographic Use Location service tag number for the Hardware; model and model numbers; the current version of the operating environment You are using; and the brand names and models of any peripheral devices (such as a mouse and/or keyboard) You are using.

(E) Call For Assistance. For warranty service and support call the support telephone numbers provided upon purchase of Your Software Support and Maintenance.

(F) Explain Your Problem to the Technician. Now You are ready to describe the problem You are having with Hardware. Let the technician know what error message You are getting and when it occurs; what You were doing when the error occurred; and what steps You may have already taken to solve the problem.

(G) Cooperate with the Technician. Experience shows that most system problems and errors can be corrected over the phone as a result of close cooperation between the user and the technician. Listen carefully to the technician and follow the technician's directions.

(H) Software/Data Backup. If the technician is unable to resolve the problem over the phone and determines that onsite support services as identified in Section 5, above, is necessary, the following standard procedure applies:

Software/Data Backup. You understand and agree that Veritas and its licensors are not responsible for any loss of software or data. You should back up the software and data on the hard disk drive of Your Hardware and on any other storage device(s) in the Hardware.

8. **HARDWARE WARRANTY SERVICE RESTRICTIONS/EXCLUSIONS.** The warranties contained in this Warranty Agreement will not apply to any-Hardware which:

a) has been altered, supplemented, upgraded or modified in any way not authorized by Veritas;
b) has been repaired except by Veritas or its designee;

Additionally, the warranties contained in this Warranty Agreement do not apply to repair or replacement caused or necessitated by: (i) events occurring after risk of loss passes to You such as loss or damage during shipment; (ii) acts of God including without limitation natural acts such as fire, flood, wind earthquake, lightning, or similar disaster; (iii) improper use, environment, installation or electrical supply, improper maintenance, or any other misuse, abuse or mishandling (such as, but not limited to, use of incorrect line voltages, use of incorrect fuses, use of incompatible, defective, or inferior devices, supplies, or accessories, improper or insufficient ventilation, or failure to follow operating instructions) by anyone other than Veritas (or its representatives); (iv) governmental actions or inactions; (v) strikes or work stoppages; (vi) Your failure to follow applicable use or operations instructions or manuals; (vii) Your failure to implement, or to allow Veritas or its designee to implement, any corrections or modifications to the Hardware made available to You by Veritas; (viii) the moving of the Hardware from one Geographic Use Location to another or from one entity to another or (ix) such other events outside Veritas's reasonable control.

9. **WARRANTY DISCLAIMERS. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, AND EXCEPT TO THE EXTENT THIS WARRANTY DISCLAIMER CONFLICTS WITH ANY WARRANTIES EXPRESSLY STATED IN THE APPLICABLE GSA SCHEDULE, THE WARRANTIES SET FORTH IN SECTION 4 ARE YOUR EXCLUSIVE WARRANTIES AND ARE IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. VERITAS MAKES NO WARRANTIES OR REPRESENTATIONS THAT THE HARDWARE WILL MEET YOUR REQUIREMENTS OR THAT OPERATION OR USE OF THE HARDWARE WILL BE UNINTERRUPTED OR ERROR-FREE**. **YOU MAY HAVE OTHER WARRANTY RIGHTS, WHICH MAY VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.**

10. GENERAL

10.1. **COMPLIANCE WITH APPLICABLE LAW.** You are solely responsible for Your compliance with, and You agree to comply with, all applicable laws, rules, and regulations in connection with Your use of the Hardware.

10.2. **INTERNATIONAL COMMERCE TERMS (INCOTERMS):** Delivery of all items shall be in accordance with the Agreement.

VERITAS™

Attachment 3
Business Critical Services

- **BUSINESS CRITICAL ADVANCED ACCESS**
- **BUSINESS CRITICAL SERVICES REMOTE PRODUCT SPECIALIST**
- **BUSINESS CRITICAL SERVICES – CLEARED SUPPORT/VERIFIED SUPPORT**

VERITAS™

Attachment 3
Business Critical Services

Where the terms of the following Business Critical Services Certificates issued separately to the Customer conflict with the terms of the Attachment 3 Certificates, the terms of the following Certificates shall control for each respective Business Critical Services support offering:

VERITAS™

Business Critical Advanced Access

- **BCS-AA Offering:** Commencing on the issue date set forth on the face of this Certificate, Veritas will provide to Licensee BCS-AA for the Product Family/Families (as defined below) listed on the face of this Certificate, under the terms and conditions listed below, until the end date set forth on the face of the Certificate.

- **Product Family:** The following URL http://go.veritas.com/bcs-aa-coveragehttp://go.veritas.com/bcs-aa-coverage lists, by Product Family, the underlying Veritas software products ("Software") eligible for coverage under BCS-AA. Licensee acknowledges that BCS-AA only applies to Software under the specific Product Family for which Licensee has purchased BCS-AA and that the list of Software may be revised and updated by Veritas from time to time without notice to Licensee. If additional Veritas software is added to the list of Software after the issue date set forth on the face of the Certificate, for the Product Family covered under this Certificate, no additional BCS-AA fee shall apply for BCS-AA coverage of such additional Software.

- **BCS-AA Services:** BCS-AA for each Product Family purchased by Licensee consists of the following services. Such services will be provided during each annual term for applicable Eligible Software: (i) priority call queuing; (ii) direct access to a Senior Veritas Technical Services Engineers for Severity 1 and Severity 2 Cases; (iii) access to the Business Critical Services website.; and (iv) unlimited number of Designated Contacts per Product Family. Delivery of BCS-AA services is in English.

- **Renewal Term; Fees for Renewal Term**. Unless otherwise terminated, Licensee's annual subscription for BCS-AA may be renewed for additional periods of twelve (12) months each (each, a "Renewal Term"), subject to general availability of BCS-AA on the applicable GSA price list and subject to Licensee's satisfaction of all requirements set forth in this Certificate. If Licensee purchases the Renewal Term through a Veritas authorized reseller, then the amount of fees for Licensee's Renewal Term and payment terms will be those fees and terms that are separately arranged between Licensee and such distributor/reseller.

II. **Prerequisites for BCS-AA:**

- **Required Maintenance/Support.** Licensee may only subscribe to receive BCS–AA (as defined in Section I above) during such time as Licensee has and maintains a valid support agreement for Essential Support for the Software. Designated Contacts shall be established in accordance with any then current Veritas policies. Additionally, Licensee is required to maintain consistency across all Software within a Product Family and may not exclude any individual Software product within a Software Family for coverage under this Certificate.

- **Payment**. Licensee's right to receive BCS-AA is subject to payment of applicable annual fees for both all required Essential Support and such BCS-AA. If Licensee's failure to pay the BCS-AA fees constitutes a material breach of the contract, then Veritas shall have the right to suspend or terminate the provision of BCS-AA for the Eligible Software. If Licensee's failure to pay for required Essential Support constitutes a material breach of the contract, then Veritas shall also have the right to suspend or terminate the provision of Essential Support for such unsupported Eligible Software, and in which case Veritas may also suspend or terminate BCS-AA for that Eligible Software. A material breach shall be deemed to occur if the Licensee fails to pay the contractually specified BCS-AA fees and/or Essential Support fees without justification for a period of sixty (60) days or more from the date when payment was due. If Licensee has a site license then Licensee is required to maintain Essential Support for all Software covered under a site license. The requirements in this Certificate to maintain and pay for Essential Support for the Eligible Software are separate from and do not change Licensee's obligation to maintain and pay for Essential Support for Software under any other agreement between Veritas and Licensee.

III. **Terms and Conditions:**

- **Limitations.** Notwithstanding anything to the contrary herein, Licensee shall have no right to sell, resell, outsource, or otherwise transfer the benefits of BCS-AA to any third party under any circumstances. Licensee shall not assign, delegate, or subcontract any of its rights or obligations under this Certificate absent Veritas's written consent, except to the extent expressly permitted under the License Agreement.

- **Termination**. Veritas may terminate Licensee's BCS-AA under this Certificate for Licensee's non-payment pursuant to Section II of this Certificate. Licensee's BCS-AA under this Certificate will also automatically terminate upon any termination of the License Agreement or any termination of required Essential Support pursuant to Section II of this Certificate. No refund will be due for any termination of BCS-AA under this Certificate. **Acknowledgement of Use of Personal Data**. Licensee recognizes that Veritas will require Licensee to supply certain personal data (such as business contact names, business telephone numbers, business e-mail addresses), in order for Veritas to provide BCS-AA and to keep Licensee apprised of support and product updates. Licensee acknowledges that Veritas is a global organization, and such personal data may be accessible on a global basis to enable Veritas to provide BCS-AA. By providing such personal data, Licensee consents to Veritas using, transferring and processing this personal data on a global basis for the purposes described **above.**

BUSINESS CRITICAL NATIONAL PACKAGE

Intentionally Deleted

I.

VERITAS™

BUSINESS CRITICAL SERVICES DATACENTER PACKAGE

Intentionally Deleted

VERITAS™

BUSINESS CRITICAL SERVICES REMOTE PRODUCT SPECIALIST

I. BCS-RPS Offering

Commencing on the issue date set forth on the face of this Certificate, Veritas will provide to Licensee BCS-RPS for the Product Family/Families (as defined below) listed on the face of this Certificate, under the terms and conditions listed below, until the end date set forth on the face of the Certificate.

- **Product Family**: The following URL http://go.veritas.com/bcs-rps-coverage lists, by Product Family, the Software eligible for coverage under BCS-RPS. Licensee acknowledges that BCS-RPS only apply to Software under the specific Product Family for which Licensee has purchased BCS-RPS and that the list of Software may be revised and updated by Veritas from time to time without notice to Licensee. If additional Veritas software is added to the list of Software after the issue date set forth on the face of the Certificate, no additional BCS-RPS fee shall apply for BCS-RPS coverage of such additional Software provided that Licensee has purchased BCS-RPS for the relevant Product Family.

- **BCS-RPS Services**: BCS-RPS for each Product Family purchased by Licensee consists of the following services. Such services will be provided during each annual term for applicable Software: (i) six (6) Designated Contacts per Product Family; (ii) Priority Call Queuing; (iii) Access to a Shared or Dedicated Remote Product Specialist, as such terms are defined at http://go.veritas.com/bcs-service-descriptions during regional business hours. All calls will be directed to an advanced team outside of regional business hours or in the event the Remote Product Specialist is not availabl.

- **Renewal Term; Fees for Renewal Term**. Unless otherwise terminated, Licensee's annual subscription for BCS-RPS may be renewed for additional periods of twelve (12) months each (each, a "Renewal Term"), subject to general availability of BCS-RPS on the applicable GSA price list and subject to Licensee's payment of the applicable BCS-RPS fees as well as payment of the annual fees for required Essential Support. If Licensee purchases the Renewal Term through a Veritas authorized reseller, then the amount of fees for Licensee's Renewal Term and payment terms will be those fees and terms that are separately arranged between Licensee and such reseller.

II. Prerequisites for BCS-RPS:

- **Required Maintenance/Support**. Licensee may only subscribe to receive BCS–RPS (as defined in Section I above) during such time as Licensee has and maintains a valid support agreement for Essential Support for the Software. BCS-RPS is only applicable to Software installed in production environments.

- **Payment**. Licensee's right to receive BCS-RPS is subject to payment of applicable annual fees for both all required Essential Support and such BCS-RPS. If Licensee's failure to pay the BCS fees constitutes a material breach of the contract, then Veritas shall have the right to suspend or terminate the provision of BCS-RPS for the Eligible Software. If Licensee's failure to pay for required Essential Support constitutes a material breach of the contract, then Veritas shall also have the right to suspend or terminate the provision of Essential Support for such unsupported Eligible Software, and in which case Veritas may also suspend or terminate BCS-RPS for that Eligible Software. A material breach shall be deemed to occur if the Licensee fails to pay the contractually specified BCS fees and/or Essential Support fees without justification for a period of sixty (60) days or more from the date payment was due. If Licensee has a site license then Licensee is required to maintain Essential Support for all Software covered under a site license. The requirements in this Certificate to maintain and pay for Essential Support for the Software are separate from and do not change Licensee's obligation to maintain and pay for Essential Support for Software under any other agreement between Veritas and Licensee.

III. Terms and Conditions:

- .

- **Designated Contacts**: Any Designated Contact may call Veritas for assistance; provided that Designated Contacts can only request BCS- RPS for Software. Designated Contacts shall have a thorough understanding of the Software for which they are the named contact(s). Veritas reserves the right to request replacement of any Designated Contact if Veritas reasonably deems that such Designated Contact lacks the necessary technical and product knowledge to assist Veritas with the timely resolution of a Licensee problem. Licensee will use its best efforts to designate a replacement Designated Contact with appropriate technical and product knowledge as soon as is reasonably practicable. Licensee recognizes that the lack of suitably-qualified Designated Contacts may affect Veritas's ability to provide the BCS-RPS hereunder.

- **Limitations**. Notwithstanding anything to the contrary herein, Licensee shall have no right to sell, resell, outsource, or otherwise transfer the benefits of BCS-RPS to any third party under any circumstances. Licensee shall not assign, delegate, subcontract any of its rights or obligations under this Certificate absent Veritas's written consent, except to the extent expressly permitted under the License Agreement.

- **Termination**. Veritas may terminate Licensee's BCS-RPS under this Certificate for Licensee's non-payment pursuant to Section II of this Certificate. Licensee's BCS-RPS under this Certificate will also automatically terminate upon any termination of the License Agreement or any termination of required Essential Support in accordance with Section II. Except as otherwise provided herein, no refund will be due for any termination of BCS-RPS under this Certificate.

- **Acknowledgement of Use of Personal Data**. Licensee recognizes that Veritas will require Licensee to supply certain personal data (such as business contact names, business telephone numbers, business e-mail addresses), in order for Veritas to provide BCS-RPS and to keep Licensee apprised of support and product updates. Licensee acknowledges that Veritas is a global organization, and such personal data may be accessible on a global basis to enable Veritas to provide BCS-RPS. By providing such personal data, Licensee consents to Veritas using, transferring and processing this personal data on a global basis for the purposes described above.

Veritas Business Critical Services – Cleared Support Services
Verified Support

I. **CSS-VS Services:** Commencing on the issue date set forth on the face of this Certificate, Veritas will provide to Licensee CSS-VS Services for the Supported Products (as defined below), listed on the face of this Certificate, for the period set forth on the face of this Certificate ("Term").

- **CSS-VS Services.** CSS-VS Services shall mean: (i) support services consisting of initial verification of Licensee' entitlement and subsequent remote diagnostic and troubleshooting performed only by United States citizens in the fifty (50) states of the United States and (ii) performed at up to a total of three (3) Supported Data Centers as designated in writing by Licensee to Veritas.

- **Supported Products.** The following URL http://go.veritas.com/cleared-support-services lists, the Supported Products, for which CSS-VS Services are provided under this Certificate, subject to purchase by Licensee of Essential Support for each Product Title designated by Licensee to be covered hereunder. Licensee acknowledges that the list of Supported Products may be revised and updated by Veritas from time to time without notice to Licensee.

- **Renewal Term; Fees for Renewal Term.** Unless otherwise terminated, upon request, Licensee's annual subscription for CSS-VS Services may be renewed for additional periods of twelve (12) months each (each, a "Renewal Term"), subject to general availability of CSS-VS Services on the applicable GSA price list and subject to Licensee's satisfaction of all requirements set forth in this Certificate. In the event the Ordering Activity wishes to renew such CSS-VS Services, the CSS-VS fees charged to such Ordering Activity or to a Veritas authorized distributor/reseller, as applicable, for each twelve (12) month period of any Renewal Term, shall be the BCS fees for the immediately preceding twelve (12) month period ("Base CSS-VS Services Fee") plus an increase not to exceed more than three percent (3%) over the Base CSS-VS Services Fee. If Licensee purchases the Renewal Term through a Veritas authorized distributor/reseller, then the amount of fees for Licensee's Renewal Term and payment terms will be those fees and terms that are separately arranged between Licensee and such distributor/reseller.

II. Prerequisites for CSS-VS Services:

- **Required License Agreement and Maintenance/Support.** Licensee must hold a valid license agreement ("License Agreement") for the underlying Software Product Title and have a current support agreement for Essential Support for each Software Product Title. Designated Contacts for CSS-VS Services shall be those same Designated Contacts established in connection with Essential Support for each Product Title designated by Licensee for coverage hereunder.

- **Payment.** Licensee's right to receive CSS-VS Services is subject to payment of applicable annual fees for (i) all required Essential Support and (ii) CSS-VS Services. If Licensee's failure to pay the BCS fees constitutes a material breach of the contract, then Veritas shall have the right to suspend or terminate the provision of CSS-VS for the Supported Products. If Licensee's failure to pay for required Essential Support constitutes a material breach of the contract, then Veritas shall also have the right to suspend or terminate the provision of Essential Support for such unsupported Product Titles, and in which case Veritas may also suspend or terminate CSS-VS for such Suport Products. A material breach shall be deemed to occur if the Licensee fails to pay the contractually specified BCS fees and/or Essential Support fees without justification for a period of sixty (60) days or more from the date payment was due.

III. Terms and Conditions:

- **Limitations.** Licensee shall have no right to sell, resell, outsource, or otherwise transfer the benefits of CSS-VS Services to any third party under any circumstances. Licensee shall not assign, delegate, or subcontract any of its rights or obligations under this Certificate absent Veritas's written consent, except to the extent expressly permitted under the License Agreement.

- **Termination.** Licensee's CSS-VS Services may be terminated (i) by Veritas for Licensee's non-payment of applicable fees in accordance with Section II; or (ii) automatically upon any termination of the License Agreement or any termination of required Essential Support in accordance with Section II. No refund will be due for any termination of CSS-VS Services.

- **Acknowledgement of Use of Personal Data.** Licensee recognizes that Veritas will require Licensee to supply certain personal data (such as business contact names, business telephone numbers, business e-mail addresses), in order for Veritas to provide CSS-VS Services and to keep Licensee apprised of support and product updates. Licensee acknowledges that Veritas is a global organization, and such personal data may be accessible on a global basis to enable Veritas to provide CSS-VS Services. If and by providing such personal data, Licensee consents to Veritas using, transferring and processing this personal data on a global basis for the purposes described above.

Veritas DeepSight Early Warning Services Certificate
Silver, Gold, and Platinum Services
Intentionally Deleted

Veritas DeepSight Early Warning Services Certificate

DeepSight Early Warning Services Starter Pack, DeepSight Early Warning Services Advanced Pack, DeepSight Early Warning Services Add-on to MSS and DeepSight DataFeeds Early Warning Services User Add-on Services

Intentionally Deleted

.

Attachment 4
Managed Security Services

Intentionally Deleted

VERITAS

SUBSCRIPTION SOFTWARE ADDENDUM

Customer Company Name:	**General Services Administration**
Title and/or Effective Date of Master Agreement:	Master License Agreement to Carahsoft Technology Corp. GSA Schedule 70 GS-35F-0119Y
Veritas Agreement Number (VAN) of Primary Agreement: **Veritas Agreement Number (VAN) of this Addendum:**	MLA110631.01 SUB110632.01
"Effective Date" of this Addendum:	April 4, 2023

This Addendum is entered into by and between the Customer identified above ("**Customer**"), and Veritas, defined as each of the Veritas entities signing this Addendum (individually, "**Veritas**"), under the Primary Agreement referenced above ("**Agreement**"), the terms of which are incorporated by reference.

The following Subscription Software terms shall supplement the terms of the Agreement:

1. Maintenance/Support. Subscription Software includes related Maintenance/Support as reflected in the Certificate. Maintenance/Support is provided and performed subject to Veritas' then-current terms, policies and processes.

2. Licensed Quantity; Subscription Term. The quantity of Subscription Software licensed to Customer ("**Licensed Quantity**") and the term of a Subscription Software entitlement ("**Subscription Term**") are as set forth in the Certificate.

3. Pricing Benefit. The following pricing benefit is available for Subscription Software licensed for at least a three (3) year term: Provided the relevant Agency Contracting Officer approves based on the type of contract, during an initial Subscription Term, orders may be submitted for additional quantities of the same Subscription Software product at the same pricing as the initial subscription pricing, prorated for the portion of that Subscription Term remaining at the time the additional quantity is added. The Subscription Term for any additional Subscription Software will terminate on the same date as the initial subscription. Customer is required to enable or submit reporting pursuant to Section 5 and otherwise be in compliance with the Agreement in order to receive this pricing benefit. This pricing benefit does not apply to promotional or one-time incentive pricing or to Appliance Software. For purposes of this section, "Appliance Software" means Subscription Software that is (1) separately licensed by Veritas as "appliance software" and/or (2) pre-loaded, pre-installed or included as a media kit accompanying a hardware appliance unit sold as a Veritas Appliance or as part of a Veritas appliance solution (such as Flex Scale software).

4. Grace Capacity; Periodic Reviews. The following terms apply to Subscription Software licensed for at least a three (3) year term:

a) Each Subscription Software license purchase includes a growth allowance of the greater of (i) ten percent (10%) of the Licensed Quantity (rounded up to the next full unit) or (ii) one (1) unit of the Subscription Software ("**Grace Capacity**"). Customer is required to enable or submit reporting pursuant to Section 5, participate in Periodic Reviews and otherwise be in compliance with the Agreement to receive the Grace Capacity.

b) Customer will participate in an annual review of its Subscription Software usage during the Subscription Term ("**Periodic Review**"). An interim review may also be triggered by use of Subscription Software in excess of the Grace Capacity or exceptional usage of the Subscription Software.

c) If Customer's use of the Subscription Software during the relevant measurement period exceeds the Licensed Quantity plus the Grace Capacity, then Customer will pay the fees associated with all usage in excess of the Licensed Quantity, pro-rated for the remainder of the Subscription Term. Pricing and term for excess usage purchases will be as set forth in Section 3. Customer will submit an Order to Veritas or customer's authorized channel partner for such excess usage promptly upon Veritas' request and/or pay any invoice for such excess usage as provided in the Agreement or the applicable terms.

5. Reporting.

(a) Automated Reporting. Customer shall enable any usage reporting mechanism or tool included in the Subscription Software and automatically upload usage reporting to Veritas for all deployed Subscription Software ("**Automated Reporting**"). If Customer cannot automatically upload usage reporting, then Customer shall manually upload Automated Reporting on each Report Due Date (as defined below).

(b) Manual Reporting. If the Subscription Software does not include a usage reporting mechanism or tool, then Customer shall provide manual reporting as described below during the Subscription Term:

i. Manual reports are due: (i) on an annual basis, no later than ninety (90) days prior to the anniversary date of the first day of the Subscription Term or a Periodic Review, if applicable; and (ii) no later than thirty (30) days after a written request for a manual report from Veritas (each, a "**Report Due Date**").

ii. Each manual report shall identify the following information on a cumulative basis, with respect to the Subscription Software: the product name (including license type), version number, quantity of each product/amount of capacity deployed, hardware model, and the regional location of the computer on which each such copy is installed.

iii. All manual reporting shall be submitted to Usage.Analytics@veritas.com or any successor address.

iv. The rights and obligations in Sections 4 and 5 are in addition to Veritas' audit and verification rights included in the Agreement.

6. Subscription Software Orders; Termination.

a) Orders. Subscription Software fees are based on Licensed Quantity and not actual usage. Licensed Quantity of Subscription Software cannot be decreased during the relevant Subscription Term. Multi-year Subscription Terms may be invoiced annually, as agreed by the parties.

b) Termination. In the event of a termination for convenience, all paid annual software subscription fees will not be prorated and no refund shall be provided. In the event of any termination of this Addendum with the Agreement, the survival terms of the Agreement shall apply; provided, however, that notwithstanding anything to the contrary in the Agreement, Customer's payment obligations for all outstanding Subscription Software Orders, including installment payments, and the audit and verification rights in the Agreement shall also survive to the extent permitted by applicable law. In no event will termination relieve Customer of its obligation to pay any fees due or payable to Veritas for the period prior to the effective date of termination.

7. **Limitation of Liability – Subscription Software**. Section 11, "Limitation of Liability" shall be amended as follows to apply to any claims arising from Subscription Software. In the second sentence, insert "OR THE FEES PAID OR OWED DURING THE PRECEDING TWELVE (12) MONTH PERIOD FOR THE SUBSCRIPTION SOFTWARE GIVING RISE TO THE CLAIM." at the end of the second sentence.

8. **Miscellaneous.** Capitalized terms used in this Addendum have the meanings given, and plural and possessive terms will be interpreted accordingly. In the event of a conflict between the Agreement and the terms of this Addendum, the terms of this Addendum shall prevail.

Veritas Alta^{TM} SaaS Protection

August 2024 Service Description

Service Overview

The Veritas Alta SaaS Protection service ("Service") consists of cloud-native software running in Microsoft Azure datacenters as a Software-as-a-Service (SaaS) offering. The Service is provided through a combination of installable software components and the Tenant to enable backup, recovery, eDiscovery, archiving, analytics, and tiering of data with the Customer's target applications and infrastructure.

This Service Description, with any attachments included by reference, is part of any agreement which incorporates this Service Description by reference (collectively, the "Agreement"), for those Services which are described in this Service Description and are provided by Veritas.

Service Offerings

Service Features

Veritas provides the following package options based on customer backup and data management needs. A customer must purchase the same package option across all their licenses.

	Enterprise	Enterprise Plus
Data Protection		
Data source connectors[1] Customer can protect its workloads through secured connections by use of data source connectors. More details in the Connector Types section.	●	●
Custom backup policies Customer can set backup scope and schedules according to its needs.	●	●
Automated backups Users enroll into scheduled backups that occur automatically.	●	●
Restore levels Customer can perform fine-grained and bulk recoveries according to its needs.	●	●
Restore options Backups can be recovered in-place, to a new or alternate location, across Microsoft 365 tenants, or to external destination.	●	●
Reporting and analytics The Service portal provides customer with the ability to monitor and report backup status and coverage.	●	●
Data Governance		
Legal hold Customer data can be preserved for litigation.	●	●

eDiscovery early case management Customers can create and manage cases for litigation and data privacy needs.	●	●
Metadata search Customers can search by usernames, files, folders, dates.	●	●
Full-text search Customers can search content within files.	Not available	●
Security		
Data encryption in-flight and at-rest Customer Data is encrypted using AES-256-bit encryption.	●	●
Azure AD integration Services have integrated support for MFA and SSO.	●	●
IP allowed/restricted list Customers can setup allowed or restricted IP lists.	●	●
Audit log Customers can query and report on the activity histories of users and system processes.	●	●
Compliance		
Custom retention policies Customers can apply immutable retention periods, subject to maintaining an active Service subscription.	●	●
Data residency Customers can select the Azure hosting region(s) for Customer Data.	●	●
Local redundancy (3 copies) Backups are synchronous replicated for high availability.	●	●
Geo-scale out, multi-region Customers can manage data sovereignty centrally for users from multiple geographies (requires pricing and deployment for each additional region).	Not available	●
Administration		
Role-based access control Customers can setup and control access of various types of users.	●	●
End user self-service access Customers can enable end users to browse, search, share, and retrieve their data on their own.	Not available	●
Add-On Services (subject to additional fees)		
Extra Data Backup Customers can make an additional backup of their air-gapped data to another location (three copies of the data). Unless a Customer has purchased Extra Data Backup for Azure blob under a Veritas-Hosted Tenant, Customers must have a separate cloud subscription (Azure, AWS, etc.) to provide a location for the extra data backup and is responsible for any of its cloud hosting costs associated with this backup.	●	●

Additional Storage Customers can increase the data storage capacity of their Tenant.	●	●

[1]Data source connector type(s) depends on license purchased (i.e., Exchange Online, Box, Slack, etc.)

Connector Types

Microsoft 365 Suite	• Provides backup and recovery for Exchange Online, OneDrive, SharePoint Online and Teams, as well as O365 Audit logs. • License meter is per user. • Users will count once across Exchange Online, OneDrive, SharePoint Online and Teams. • A user license includes a storage allocation of 20 GB per user.
Microsoft 365 Exchange Online	• Provides backup and recovery for mailbox items that include Email, calendar, contacts, tasks, and notes. • License meter is per user. • A user license includes a storage allocation of 10 GB per user.
Microsoft 365 OneDrive	• Provides backup and recovery for OneDrive items that include files, folders and permissions. • License meter is per user. • A user license includes a storage allocation of 10 GB per user.
Microsoft 365 SharePoint Online	• Provides backup and recovery for SharePoint items that include all list items from any content type within site collections, including permissions and all item metadata. License meter is per user. • A user license includes a storage allocation of 10 GB per user.
Microsoft 365 Teams	• Provides backup and recovery for Teams items that include Team sites, members, member permissions, channels, posts, files and wiki. • License meter is per user. • A user license includes a storage allocation of 10 GB per user.

Salesforce	• Provides backup and recovery for structured data elements (including standard and custom objects and records). • License meter is per user. • A user license includes a storage allocation of 10 GB per user.
Box	• Provides backup and recovery for Box items that include files, folders and permissions. • License meter is per user. • A user license includes a storage allocation of 10 GB per user.
Slack	• Slack provides backup and recovery for Slack items that include workspaces, channels, messages, and files. • License meter is per user. • A user license includes a storage allocation of 10 GB per user.
Google Workspace	• Provides backup and recovery for Google Mail and Google Drive items that include files, folders, and permissions. • License meter is per user. • A user license includes a storage allocation of 20 GB per user.
Entra ID (formerly Azure AD)	• Provides backup and recovery of users, groups, app registrations and enterprise applications • Ability to auto-restore relationships (with limitations) and restore deleted objects (within last 30 days) • License meter is per user • A user license includes a storage allocation of 200 MB per user.
Structured Data	• Provides backup, recovery, and archiving for small file-size workloads that are generally high in object count, thus requiring higher performance compute and storage compared to Unstructured Data workloads. • License meter is per FETB.

Unstructured Data – Cool	• Provides backup, recovery, tiering and archiving for Unstructured Data that requires immediate retrieval/access whenever necessary. • The following workloads are supported: ○ File systems: Microsoft Windows Server, Linux, UNIX ○ Object storages: Azure Blob, Azure Files, AWS S3 • License meter is per FETB.
Unstructured Data – Archive	• Provides backup and long-term archiving for Unstructured Data requires cost-efficient storage but does not need immediate retrieval response times. • The following workloads are supported: ○ File systems: Microsoft Windows Server, Linux, UNIX ○ Object storages: Azure Blob, Azure Files, AWS S3 • License meter is per FETB.

Veritas reserves the right to move Customer Data under a Per User Connector Type that has not been accessed by Customer for a year or longer to an archive tier within Azure. Any backups of Customer Data from an archive tier can still be restored but will take additional time to do so.

Service Components

Some Connector Types may require use of a Software Component. Customer's right to use such Software Component begins when the Service is activated and ends when Customer's right to use the associated Service terminates or expires. Customer must uninstall a Software Component when Customer's right to use the associated Service terminates or expires. Veritas may disable the Software Component at that time.

Shared Storage Allocation

The storage allocation for each Connector Type is aggregated within a Tenant across all Users as determined by multiplying the quantity of Users for such Connector Type by the allocation per User. The per Connector Type storage allocation is then added to the Customer's overall shared storage capacity and enforced at the Tenant level. Customers can purchase Additional Storage to increase the overall aggregate amount of storage capacity of their Tenant. FETB-metered Connector Types are enforced separately per Connector Type within a Tenant on the basis of the total FETB purchased, and do not affect the shared storage capacity of per User Connector Types or other FETB-metered Connector Types.

License Enforcement

The Service alerts customers when their subscription term is about to expire. Once a subscription expires, new backups will suspend and not resume until the subscription is renewed. Otherwise, Customer Data will be decommissioned in accordance with the Data Decommissioning section.

Service Subscriptions are metered on either a per User or per FETB basis, as described in the Connector Types section above. If there are multiple connectors that are set up, usage is aggregated at the Tenant level to get the total capacity used by the connectors configured.

- For connectors with user-based licenses, the Service will alert the customer when 100% of available licenses and/or storage are used. The service will not allow more users to be added to the connector's scope once a connector has used all available licenses. New backups will be suspended and will not run until Customer either reduces capacity usage or purchases more storage.

- For connectors with user-based licenses there are limits on capacity allocated. The service will alert the customer when the data protected by the Service for a particular license type has reached 80% capacity, 90% capacity and 100% capacity or exceeds available capacity, as compared against the Shared Storage Allocation. The Service will not allow more users to be added to the connector's scope, and new backups will be suspended and will not be run until Customer either reduces capacity usage or purchases more storage.

- For connectors with front-end terabyte-based licenses, the Service will alert the customer when data protected by the Service for a particular license type has reached 80% capacity, 90% capacity, and when at 100% capacity or exceeds available capacity. Once the 100% or exceeds capacity alert is triggered, new backups will be suspended and will not be run until Customer either reduces capacity usage or purchases more licenses.

- Licenses are time-bound according to Customer's Service Subscription start and end dates. If Customer's Subscription expires, Customer will no longer have access to login to the Tenant and new backups will be suspended, and all Customer Data will be decommissioned in accordance with the Data Decommissioning section, including data with immutable retention periods or on legal hold.

Customer Responsibilities

Veritas can only perform the Service if Customer provides required information or performs required actions. If Customer does not provide/perform per the following responsibilities, Veritas's performance of the Service may be delayed, impaired, or prevented and/or eligibility for Service Level Agreement benefits may be voided, as noted below.

- Setup Enablement: Customer must provide information required for Veritas to begin providing the Service.

- Customer Configurations vs. Default Settings: Customer must configure the features of the Service through the web portal interface, if applicable, or default settings will apply. In some cases, default settings do not exist, and no

Service will be provided until Customer chooses a setting. Configuration and use of the Service(s) are entirely in Customer's control.

- Configuration: Should a Service be suspended or terminated for any reason whatsoever, Veritas shall reverse all configuration changes made upon provisioning the Service and it shall be the responsibility of Customer to undertake all other necessary configuration changes when the Service is reinstated.

- Adequate Customer Personnel: Customer must provide adequate personnel to assist Veritas in delivery of the Service, upon reasonable request by Veritas.

- Web Interface Service Portal Access: Customer can access the Service portal by using a secure password protected login. The Service portal provides the ability for Customer to configure and manage the Service, access reports, and view data and statistics when available as part of the Service. Customer must configure the features of the Service through the Service portal or default settings will apply. In some cases, default settings do not exist, and no Service will be provided until Customer chooses a setting. Configuration and use of the Service are entirely in Customer's control.

- Security: Customer shall perform commercially reasonable efforts, using procedures, third-party software, and the security features of the Service, to maintain the security of Customer Data.

- Compliance: Customer is responsible for all activities that occur in User accounts and for its Users' compliance with the Agreement and with the Acceptable Use Policy available at https://www.veritas.com/company/legal/acceptable-use-policy. If Customer becomes aware of a User's violation of the Agreement or Acceptable Use Policy, Customer must notify Veritas as soon as reasonably practicable.

- Security Vulnerability or Incident. If Customer becomes aware of any actual or potential security vulnerability or incident, Customer must immediately report it to Veritas through the process set forth at https://www.veritas.com/security or successor address.

Service-Specific Terms

Fair Use

Customers using the Service are expected to perform data operations and egress in line with normal and reasonable industry standards of similar services. Activities that fall outside of these reasonable standards include without limitation:

- data egress for purposes other than data recovery or responses to reasonable data privacy or eDiscovery requests

- egress of all data to populate another repository or because of Service cancellation

- excessive testing of backup or restoration capabilities

In the event Customer's use of the service involve activities as described above or exceed the egress thresholds in the table below by any number of terabytes or portion thereof, Veritas reserves the right to invoice for such excess use or suspend the service until Customer can conform its use of the service.

Veritas Alta SaaS Protection Offering	Maximum terabytes of egress per year as a % of the total pooled FETB purchased.
Unstructured files – Archive	3%
All other offerings	20%

As an example, a customer may have purchased several Veritas Alta SaaS Protection services and the resulting pooled storage allocation equals 100 terabytes. Under the fair use policy, the customer can egress up to 20 terabytes in an annual period (no carryover) without incurring additional fees: 100 terabytes * 20% maximum egress = 20 terabytes.

Assistance and Technical Support

Customer Assistance. Veritas will provide the following assistance as part of the Service:

- Receive and process orders for implementation of the Service
- Receive and process requests for permitted modifications to Service features; and
- Respond to billing and invoicing questions

Technical Support. The following technical support ("Support") is included with the Service.

- Support available on a twenty-four (24) hours/day by seven (7) days/week basis to assist Customer with configuration of the Service features and to address issues and questions with the Service.

Maintenance. Veritas must perform maintenance on the Service Infrastructure in order to provide the Service in accordance with the Agreement. The following applies to such maintenance:

- *Planned Maintenance*. "**Planned Maintenance**" means scheduled maintenance periods which during which Service may be disrupted or prevented due to non-availability of the Service Infrastructure. Veritas' standard Planned Maintenance time(s) are listed below. Veritas will use commercially reasonable efforts to perform Planned Maintenance at times when collective customer activity is low, in the time zone in which the affected Infrastructure is located, and only on part, not all, of the network. If possible, Planned Maintenance will be carried out without affecting the Service. During Planned Maintenance, Service may be diverted to sections of the Infrastructure not undergoing maintenance in order to minimize disruption of the Service.

  - Veritas performs a weekly Planned Maintenance beginning at 12am GMT on Sundays and typically lasting for 2 hours or less. Customers that would like to alter this Planned Maintenance window will need to call Support to see if reasonable accommodations can be made.
  - For any other Planned Maintenance outside of the above time(s), Veritas will use commercially reasonable efforts to give Customer five (5) calendar days' notification via the Service.
- *Emergency Maintenance.* "**Emergency Maintenance**" means unscheduled maintenance periods which during which Service may be disrupted or prevented due to non-availability of the Service Infrastructure or any maintenance for which Veritas could not have reasonably prepared for the need for such maintenance, and failure to perform the maintenance would adversely impact Customer. Where Emergency Maintenance is necessary and is likely to affect the Service, Veritas will endeavor to inform the affected parties in advance via email, or SMS or by phone no less than one (1) hour prior to the start of the Emergency Maintenance.

Automatic Renewal and Service Cancellation

T Renewal of the Service is in accordance with Section 5 of the Addendum. The Service may be renewed by the Customer executing a written Order for the Renewal Period.

Please note that if Customer has opted out of auto-renewal at the time of purchase ("DNR"), Customer will be responsible for submitting a timely renewal order. Any processing delays, late renewals, channel issues or other problems with the renewal order may cause the Service to expire and any Customer Data stored by the Service shall be deleted in accordance with the Data Decommissioning section. Not submitting a timely renewal order is deemed the same as a cancellation notice, and Customer Data and the Customer Tenant will be permanently deleted in accordance with the Data Decommissioning section.

Automatic renewals are subject to a renewal uplift, except that any renewal order of a DNR purchase or purchase provided under a promotional discount is subject to the then-current pricing.

Data Decommissioning

Customer Data will be decommissioned in the following events, or as otherwise set forth in this Service Description:

- Service cancellation (either by request of Customer or in the event of non-payment)
- Service termination or expiration
- License reduction at renewal in excess of 10%

Customer loses all access to the Service and its Customer Data, and no new backup jobs will be performed immediately following suspension, expiration, or termination of Services.

Unless otherwise prohibited by law or court order, decommissioned Customer Data will be deleted in accordance with our standard deletion practices within thirty (30) days of the Data Decommissioning event and is irretrievable thereafter.

If Customer needs a copy of their Customer Data, Customer should continue subscribing to the Service until such time as Customer has retrieved all Customer Data through self-service data exports.

Overages

If Customer's actual usage exceeds its contracted quantity, then Veritas will invoice for excess Service use and Customer will promptly pay for such excess use. In such an event, Veritas will charge fees for the excess use at the same rates for the current Term monthly in arrears or in accordance with Veritas' then-current processes.

Usage Reduction

Customer cannot reduce the agreed upon quantity of users or FETB during any existing term but may only reduce that quantity at renewal time. Absent evidence of a company divestiture, split or other entity realignment, Veritas reserves the right to reduce the quantities for the existing product(s) as a one-time courtesy by no more than ten percent (10%) of the existing amount at any given renewal time or as otherwise set forth in Veritas' then-current processes. Pricing will be adjusted for the lower volume which shall result in increased per user pricing, and prior discounting will not be available. Customer Data associated with the removed licenses will not be decommissioned but will count toward Customer's adjusted Shared Storage Allocation based on the new user and FETB quantities.

Additional Service Requirements

- Customer shall comply with all applicable laws with respect to use of the Service(s). In certain countries it may be necessary to obtain the consent of individual personnel. Configuration and use of the Service(s) is entirely in Customer's control, therefore, Veritas is not liable for Customer's use of the Service(s), nor liable for any civil or criminal liability that may be incurred by Customer as a result of the operation of the Service.

- Veritas may update the Service at any time in order to maintain the effectiveness of the Service.

- The Service (including any Software Components) may use open source and other third-party materials that are subject to a separate license. Please see the applicable Third-Party Notice, if applicable, at https://www.veritas.com/about/legal/license-agreements.

- Legacy Service Offerings: Service offerings listed in this Service Description are the ones generally available to new customers. For existing customers who may still be actively using a Service offering not detailed herein, please see https://www.veritas.com/content/dam/Veritas/docs/policies/Veritas_Alta_SaaS_Protection_Legacy_Service_Description.pdf for additional details on such Services.

- If Customer has not provided the requested provisioning information to allow Veritas to provide the Service, Veritas reserves the right to begin charging for the Service within thirty (30) days of receipt of an order for the Service.

Service Level Agreement ("SLA")

Veritas' Service Level Agreement is dependent on availability of the third-party cloud provider resources and is only available for customers where the Tenant is hosted in the Veritas Azure environment (i.e., a Veritas-Hosted Tenant).

- Veritas' Service Level Agreement shall provide 99.9% or higher Uptime for the Service.

- "Uptime" is defined as the time during which a Customer is able to Access the Service, as reported by the Veritas incident management system. "Access" is defined as a Customer being able to successfully login and use the Service functionality, as outlined in this Service Description.

- Uptime is measured every calendar month as a percentage value. The monthly Uptime percentage is the total number of minutes of Uptime achieved in a calendar month, divided by the total number of minutes in a calendar month.

Exclusions

- This SLA will not operate: (i) during periods of Planned Maintenance or Emergency Maintenance, periods of non-availability due to force majeure or acts or omissions of either Customer or a third party; (ii) due to overall internet congestion, slowdown or unavailability; (iii) bandwidth or other limitations caused by Customer internet service provider (ISP); (iv) unavailability of generic internet services (e.g. DNS servers); (v) a result of Customer equipment or third party computer hardware, software or network infrastructure not within the sole control of Veritas; (vi) during any period of suspension of service by Veritas in accordance with the terms of the Agreement; (vii) where Customer is in breach of the Agreement (including without limitation if Customer has any overdue invoices); or (viii) Customer has not configured the Service in accordance with the Agreement.

Service Credits

- If the Service does not meet the stated SLA, Customer may submit a Service Credit Request for a Service Credit. Service Credits are calculated as follows:

Availability	Service Credit[1]
≥=99.9%	0%
>=99.0% but <99.9%	10%
<99.0%	25%

[1] Service Credits are calculated as a percentage of the monthly cost of the service when the outage occurred (regardless of licensing model). Service Credit percentages in the table above are an aggregate maximum for all SLA claims for a single Service in a given calendar month. Service Credits only apply if the Customer's account is current and not suspended for non-payment or other non-compliance with terms. Service Credits are provided to the party receiving the Veritas invoice.

- To successfully claim a Service Credit, Customer must submit a Service Credit Request within fifteen (15) business days of the end of the calendar month in which the suspected SLA non-compliance occurred. The request must specify which service was impacted, and the dates and times of service unavailability.

- Veritas will validate the information provided by the Customer and if a Service Credit is due, it will be applied against the next Veritas invoice for the Customer's Service. If a Service Credit is successfully claimed for more than one Veritas Service, then the quantity will equal the number of credits applied and the total will be aggregated to reflect the total value of the Service Credits claimed in that measurement period.

- The remedies set out in this SLA shall be Customer's sole and exclusive remedy in contract, tort (including without limitation negligence) or otherwise, with respect to this SLA.

Data Privacy

Data Collection; Data Protection Regulations. In connection with Customer's use of the Service, Veritas and Veritas' licensors, subcontractors, or agents on Veritas' behalf may collect, retain, disclose and use certain information ("Collected Data"). Collected Data may include, but is not limited to, personally identifiable information about Customer, Customer's devices or systems or Customer's software usage. Veritas uses such Collected Data to enable, optimize and provide the Service and/or maintenance/support to Customer (and may engage third parties to do so as well) and to improve Veritas' products and services in general, including by reviewing aggregate data for statistical analyses. By installing and/or using the Service, Customer agrees to allow Veritas to collect Collected Data as described in this section. Please refer to Veritas' product privacy notices attached hereto and at https://www.veritas.com/company/privacy in order to fully understand what information Veritas collects, retains, discloses, and uses from Customer or Customer's devices. Please note that the use of the Service may be subject to data protection laws or regulations in certain jurisdictions. Customer is responsible for ensuring that Customer's use of the Service is in accordance with such laws or regulations. Customer acknowledges that the Collected Data will be processed and accessible on a global basis by Veritas, its Affiliates agents and subcontractors for the purposes of providing the Service and/or maintenance/support, to generate statistical information about the Service, for internal research and development, and as otherwise described in the Agreement. Customer also consents for Customer and as agent for its contacts whose details have been collected as part of the Collected Data to the use by Veritas of that personal information for the purposes of informing Customer of Veritas products and services which may be of interest to Customer and account management. Where Customer's processing of the personal data provided to Veritas under this Agreement is subject to the General Data Protection Regulation (EU) 2016/679, or other applicable laws that relate to the processing of personal data and privacy that may exist in the European Economic Area, United Kingdom, or Switzerland, Veritas shall process such personal data in accordance with the Data Processing Terms and Conditions at www.veritas.com/privacy. Veritas may disclose the Collected Data as required or permitted by law or in response to a subpoena or other legal process.

Definitions

Capitalized terms used in this Service Description, and not otherwise defined in the Agreement or this Service Description, have the meaning given below:

"**Azure**" means the Microsoft cloud infrastructure and platform offering known as "Azure".

"**Customer Data**" means the data Customer stores or archives in the Service.

"**FETB**" or "**Front-End Terabyte**" means front-end terabyte and refers to the total aggregate amount of uncompressed data in terabytes. One terabyte equals 1,024 gigabytes of data.

"**GB**" refers to the total aggregate amount of uncompressed data in gigabytes. One gigabyte equals 1024 megabytes of data.

"**Infrastructure**" means any Veritas or licensor technology and intellectual property used to provide the Services.

"**Open Source Code**" means a software program that is licensed under terms that require disclosure to parties other than the licensor of the source materials of the software program or modifications thereof, or any source materials of any other software program with which the Open Source Code software program is intended to operate, or that create obligations to distribute any portions of any software program with which the Open Source Code software program is used. Open Source Code includes, without limitation, any software licensed under the GNU General Public License.

"**Service Component**" means certain enabling software, hardware peripherals and associated documentation which may be separately provided by Veritas as an incidental part of a Service. Any additional rights and obligations with respect to the use of Service Components shall be as set forth in this Service Description.

"Service Credit" means the amount of money that will be credited to Customer's next invoice after submission of a Service Credit Request and validation by Veritas that a credit is due to Customer.

"Service Credit Request" means the SLA credit request a Customer submits to Veritas by creating a technical support case. Information on how to create a technical support case may be found at https://www.veritas.com/support/en_US.html.

"**Software Component**" means a Service Component consisting of Veritas software in object code format, as may be required by a Service, which must be installed by Customer outside of the Tenant, in order to receive the Service, or some portion thereof.

"**Subscription Instrument**" means one or more of the following applicable documents which further defines Customer's rights and obligation related to the Service: a Veritas certificate or a similar document issued by Veritas, or a written agreement between Customer and Veritas, that accompanies, precedes or follows the Service.

"**Subscription Period**" means the period beginning from execution of a Subscription Order Form and ending upon termination or cancellation of the Service.

"**Structured Data**" means data that conforms to a data model, has a well-defined structure, follow a consistent order, and can be accessed and used by a computer program. For purposes of illustration only: machine generated data, event logs, database records.

"Suite" means a collection of Veritas Alta Archiving Services sold together as detailed further in this Service Description.

"**Tenant**" means the isolated compute, storage, and networking resources and related configuration that is hosted in a cloud environment that is dedicated to Customer. A Tenant hosted by Veritas is known as a "Veritas-Hosted Tenant."

"**Unstructured Data**" means data that is not Structured Data. For purposes of illustration only: video, images, audio, user-generated files, application data, compliance records, litigation data, and public records data.

"**User**" means an individual who is authorized by Customer to use the Service.

VERITAS™

Data Processing Terms and Conditions

These Data Processing Terms and Conditions ("**Terms and Conditions**") are offered by the Veritas entity which is the contracting party to the applicable Veritas agreement(s) in effect between Veritas and Customer under which Customer procures, and Veritas provides Services (collectively and individually, the "**Agreement**") and incorporates terms in relation to the processing and the transfers of Customer Personal Data outside the European Economic Area ("**EEA**") Switzerland and United Kingdom that are offered by Veritas Technologies LLC ("**Customer Data Transfer Agreemen**t").

If the Customer is an Ordering Activity under GSA Schedule Contracts, the parties shall only be required to comply with the Federal law of the United States and the parties expressly do not agree to comply with any provision of this Data Processing Agreement, EU Law, or law of an EU Member State that is inconsistent with the Federal law of the United States.

The parties to the Agreement agree that the following terms shall apply to the processing of Customer Personal Data under the Agreement and form part of the Agreement:

1. **DEFINITIONS AND INTERPRETATIONS**: In these Term and Conditions all capitalised terms not defined herein shall have the meaning set out in the Agreement):

"Affiliate" means an entity controlled by, under common control with, or controlling a party, where control is denoted by having, (directly or indirectly), fifty percent (50%) or more of the voting power (or equivalent) of the applicable entity;
"Appropriate Technical and Organisational Measures" shall be interpreted in accordance with the requirements of the Data Protection Legislation;
"**CCPA**" means the California Consumer Privacy Act of 2018, codified at Cal. Civ. Code §1798.100 et seq , as amended by the California Privacy Rights Act, and its implementing regulations as may be amended from time to time;
"Customer Personal Data" means any Personal Data the Processing of which is subject to the Data Protection Legislation, that is disclosed by Customer and its Affiliates to Veritas to enable Veritas to fulfil its obligations under the Agreement;

"Data Controller", "Data Processor", "Data Subject", "Data Breach" and **"Supervisory Authority"** shall be interpreted in accordance with the definitions in the Data Protection Legislation;

"**Data Protection Legislation**" means all applicable data protection and privacy laws, regulations and mandatory codes of practice applicable to the Processing of Customer Personal data including the General Data Protection Regulation (EU) 2016/679 ("**EU GDPR**") and all other laws that may exist in the European Economic Area, Switzerland or United Kingdom, Canada and the United States and its states relating to the Processing of Personal Data and any legislation and/or regulation as amended, repealed, consolidated or replaced from time to time;

"Lawful Safeguards" means such legally enforceable mechanism(s) for transfers of Customer Personal Data as may be permitted under Data Protection Legislation from time to time including but not limited to the SCCs and UK IDTA (as defined below);

"Personal Data" shall be interpreted in accordance with the definitions in the Data Protection Legislation;

"Processing" shall be interpreted in accordance with the definitions in the Data Protection Legislation;

"**Sensitive Personal Data**" has the same meaning as 'special categories of data' in Data Protection Legislation;

"**Standard Contractual Clauses**" or "**SCCs**" means the standard data protection clauses for the transfer of Personal Data to third countries which do not ensure an adequate level of data protection, as described in Article 46 of the GDPR and approved by the European Commission decision 2121/914/EC, dated 4 June 2021, or any set of clauses later approved by the European Commission which amend, replace or supersede such version;

"Sell" means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, personal information to a third party for monetary or other valuable consideration;

"Service" means any service that Veritas undertakes for the Customer under the Agreement that involves the Processing of Customer Personal Data;

"**UK IDTA**" or "**UK Addendum**" means the International Data Transfer Addendum to the EU Commission SCCs as issued by the UK's Supervisory Authority (the Information Commissioner or any replacement thereof) under section 119A(1) of the Data Protection Act 2018; and

"**Veritas Companies**" means the members of the Veritas Group.

2. SCOPE

a. Customer shall be the Data Controller and Veritas shall be the Data Processor in relation to the Customer Personal Data.

b. The subject-matter and purpose of the data Processing is the performance of Veritas's obligations under the Agreement and the Processing will be carried out until the date that those obligations cease, subject to any requirements under local law. The nature and purpose of the Processing, the types of Customer Personal Data that Veritas Processes and the categories of Data Subjects whose Personal Data is Processed is set out for each Service that Veritas provides at www.veritas.com/privacy.

c. Customer warrants that the instructions it provides to Veritas in relation to the Processing of the Customer Personal Data will comply with the Data Protection Legislation and that its Processing of Customer Personal Data complies with the Data Protection Legislation.

3. PROCESSOR OBLIGATIONS

Veritas will:

a. Process the Customer Personal Data only in accordance with written instructions from Customer (which may be specific instructions or instructions of a general nature as set out in the Agreement or as otherwise notified by Customer to Veritas in writing from time to time) and not for its own purposes. If required to Process Customer Personal Data for any other purpose by European Union or Member State law to which Veritas is subject, Veritas shall inform the Customer of this requirement before the Processing commences, unless that law prohibits this on important grounds of public interest. Customer accepts that if it instructs Veritas to do something that exceeds the instructions specifically established in the Agreement, Veritas may require a reasonable additional charge to fulfil those instructions which will be as agreed in writing between the parties.

b. at Customer's request and cost, taking into account the nature of the Processing:

   i. assist Customer by taking Appropriate Technical and Organisational Measures and in so far as it is possible, in fulfilling Customer's obligations to respond to requests from Data Subjects of Customer Personal Data exercising their rights (to the extent that the Customer Personal Data is not accessible to the Customer through the Service); and

   ii. taking into account the information available to Veritas, assist the Customer in ensuring Customer's compliance with the obligations pursuant to Articles 32 to 36 of the EU GDPR or equivalent provisions in the Data Protection Legislation;

c. implement and maintain Appropriate Technical and Organisational Measures to protect the Customer Personal Data against unauthorised or unlawful processing and against accidental loss, destruction, damage, theft, alteration or disclosure. These measures shall be appropriate to the harm which might result from any unauthorised or unlawful Processing, accidental loss, destruction, damage or theft of the Customer Personal Data and having regard to the nature of the Customer Personal Data which is to be protected. As a minimum, these will include the

Technical and Organisational Measures detailed in Annex II.

d. ensure that only personnel who are contractually bound to respect the confidentiality of the Customer Personal Data have access to it for the purposes of Veritas's obligations under the Agreement;

e. not retain any of the Customer Personal Data for longer than is necessary to perform its obligations under the Agreement and, at the end of the Service or upon Customer's request, securely delete or return such Customer Personal Data to Customer in accordance with any relevant terms in the Agreement unless local law requires storage of the Customer Personal Data, and ensure that all Veritas Companies that have received relevant Customer Personal Data are made aware of any request to delete or return the relevant Customer Personal Data; and

f. upon request by the Customer, update, correct or delete any Customer Personal Data, unless Customer has the ability to carry out that action on the Customer Personal Data itself, or local law requires storage of the Customer Personal Data, and ensure that all Veritas Companies that have received relevant Customer Personal Data are made aware of any request to update, correct, or delete the relevant Customer Personal Data.

4. SUB-PROCESSING

a. Customer agrees that Veritas may transfer Customer Personal Data to Veritas Companies and the third parties listed at https://www.veritas.com/content/dam/Veritas/docs/policies/sub-processors-for-veritas-service.pdf as sub-processors for the relevant Service ("**Sub-processors**"), for the purpose of fulfilling Veritas' obligations under the Agreement. Veritas will ensure that any Sub-processors to whom Veritas transfers Customer Personal Data enter into written agreements requiring that the Sub-processor abide by provisions that are no less protective than these Terms and Conditions. Veritas will remain fully responsible to Customer for the fulfilment of its obligations under these Terms and Conditions and the Agreement. Veritas can at any time and at its discretion appoint a new Sub- processor provided that Customer is given at least fifteen (15) days' prior notice ("**Sub-processor Notice**"). If Customer has a legitimate objection to the Sub-processor, consisting of reasonable and documented grounds relating to a Sub-processor's non-compliance with applicable Data Protection Legislation, Customer shall provide written notice of such objection to Veritas during the fifteen (15) days of Veritas providing the Sub- processor Notice.

b. In order to receive Sub-processor Notices for a Service, it shall be the responsibility of Customer to email Veritas at Privacy@veritas.com with "Sub-processor Subscribe" in the subject line of the email, giving details of the Service for which Sub-processor Notices are required. It is also Customer's responsibility to notify Veritas of any changes to the email address to which Sub-processor Notices should be sent, using the same email address and subject line. Sub-processor Notices shall be sent to the email address from which the communication is sent, unless another email address for receipt of Sub-processor Notices is stipulated in the relevant email.

5. BREACH NOTIFICATION

Veritas shall notify Customer without undue delay if Veritas becomes aware of a confirmed accidental, unauthorised or unlawful destruction, loss, alteration, or disclosure of, or access to the Customer Personal Data (a "**Data Breach**"), take such reasonable steps as may be required to investigate and remedy the Data Breach and as soon as possible and where known by Veritas provide Customer with:

a. a detailed description of the Data Breach as at that time and the mitigations enacted;

b. the type and volume of Customer Personal Data that was the subject of the Data Breach;

c. the identity of each affected person, as soon as such information can reasonably be collected or otherwise becomes available as well as periodic updates to this information; and

d. any other information Customer may reasonably request relating to the Data Breach.

6. DATA TRANSFERS

a. Veritas may transfer Customer Personal Data by way of Lawful Safeguards for transfers to third countries outside the EEA, the United Kingdom and Switzerland where such transfers are normally required for the purposes of fulfilling Veritas' obligations under the Agreement. As the data importer in relation to such transfers, Veritas Technologies LLC will comply with the obligations of a data importer as set out in the Standard Contractual Clauses, as incorporated into the Customer Data Transfer Agreement, a copy of which is at Schedule 1 hereto ("**Customer Data Transfer Agreement**").

b. Where the contracting party to the Agreement is a Veritas entity other than Veritas Technologies LLC, Customer hereby authorises Veritas to enter into an agreement with Veritas Technologies LLC on the terms of Customer Data Transfer Agreement as agent for Customer and Veritas agrees to enter into such agreement with Veritas Technologies LLC forthwith.

c. If the parties are relying on the Customer Data Transfer Agreement to transfer Customer Personal Data outside the EEA, the United Kingdom or Switzerland, and the European Commission decision on Standard Contractual Clauses is held to be invalid or no longer applicable to such transfers, or if any Supervisory Authority requires transfers of Customer Personal Data made pursuant to such decision to be suspended, then Customer may, at its discretion, require Veritas to cease Processing Customer Personal Data to which this paragraph applies, or co-operate with Veritas to facilitate use of an alternative transfer, mechanism. Customer accepts that if it instructs Veritas to cease Processing the Customer Personal Data, such instruction may render it impossible for Veritas to continue to provide the relevant Service or render it impossible for the Customer to continue use of the relevant Service, and if that happens, such situation shall be treated as an event beyond Veritas' reasonable control and shall be handled in accordance with the relevant provisions in the Agreement.

7. AUDIT

a. During the term of the Agreement, and no more than once per year, Veritas will allow, on at least 30 business days' notice (unless shorter notice period is required by applicable law or statutory authority), Customer and its respective auditors or authorised agents to conduct reasonable audits or inspections to verify that Veritas is Processing Customer Personal Data in accordance with its obligations under these Terms and Conditions and applicable Data Protection Legislation.

b. Veritas may in certain circumstances provide a third-party audit report or complete questionnaires rather than permitting Customer itself to audit where Veritas believes its compliance can be verified in such a manner.

c. Veritas shall notify Customer immediately if it considers that an instruction from Customer is in breach of Data Protection Legislation, and Veritas shall be entitled but not obliged to suspend execution of the instructions concerned, until Customer confirms such instructions in writing.

8. CCPA

Customer has made Personal Data available to Veritas. Veritas agrees that Veritas (i) will not retain, use or disclose, any such Personal Data of the Customers for any purpose other than for the specific purpose of performing the Services for the Business Purposes (as defined in CCPA) of the Customer under the Agreement; and (ii) will not Sell Personal Data. Veritas confirms that it understands and will comply with these obligations.

9. MISCELLANEOUS

a. In the event of any conflict or inconsistency between the provisions of the Agreement and these Terms and Conditions, the provisions of these Terms and Conditions shall prevail. Save as specifically modified and amended in these Terms and Conditions, all the terms, provisions and requirements contained in the Agreement shall remain in full force and effect and govern these Terms and Conditions.

b. Except in relation to the Customer Data Transfer Agreement, these Terms and Conditions and any dispute or claim (including non-contractual disputes or claims) arising out of, or in connection with them or their subject matter or formation shall be governed by and interpreted in accordance with the law which governs the Agreement, and Veritas and Customer irrevocably agree that the courts that have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims) that rises out of, or in connection with, the Agreement, or its subject matter or formation, shall also have exclusive jurisdiction in relation to any disputes or claims arising from these Terms or Conditions.

SCHEDULE ONE

CUSTOMER DATA TRANSFER AGREEMENT

STANDARD CONTRACTUAL CLAUSES

The Parties have agreed on the following Standard Contractual Clauses (transfer controller to processor-Module 2) (the "Clauses") in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of personal data specified in the attached Annex I.

For the purposes of the Clauses, Customer is the data exporter and Veritas is the data importer.

In case of any transfer of Customer Personal Data where Data Protection Legislation of the UK apply to the data exporter's processing when making that transfer, the SCCs shall be read in accordance with, and deemed amended by, the provisions of Part 2 (Mandatory Clauses) of the UK IDTA and the parties confirm that the information required for the purposes of Part 1 (Tables) of the UK IDTA is set out in these Terms and Conditions.

In case of any transfer of Customer Personal Data where Data Protection Legislation of Switzerland applies to the data exporter's processing, the following will apply:

Clause 8.8(i) shall be read as the onward transfer being to a country approved by the Swiss Federal Council;

Clause 8.8(ii) appropriate safeguards shall be those approved by the Swiss Federal Council with respect to the processing in question;

Clause 11(c), references to the Supervisory Authority of the Member state shall be read as referring to the Data Protection and Information Commissioner's Office (FDPIC); and

Clause 17 shall be read as the law of Switzerland and clause 18(b) shall be the courts of Switzerland.

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex IA. (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex IA. (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex IB.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfers

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex IB.

Clause 7 – Optional

Docking clause

Reserved

SECTION II - OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex IB, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex IB. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter “personal data breach”).

In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person’s sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter “sensitive data”), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex IB.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter “onward transfer”) if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 15 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these

Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub- processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer’s responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III - LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article **23(1)** of Regulation **(EU) 2016/679,** are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination- including those requiring the disclosure of data to public authorities or authorising access by such authorities - relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.1 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV - FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority [for Module Three: and the controller] of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) [For Modules One, Two and Three]: Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data.

The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

ANNEX I

A. LIST OF PARTIES

MODULE TWO: Transfer controller to processor

Data exporter(s): Name: ...As set out in the Agreement

Address: …As set out in the Agreement

Contact person’s name, position and contact details: ... As set out in the Notices clause of the Agreement

Activities relevant to the data transferred under these Clauses: ... See section B

below

Signature and date: ...As set out in the Agreement

Role (controller/processor): Controller

Data importer(s):

1. Name: ... As set out in the Agreement

Address: ... As set out in the Agreement

Contact person’s name, position and contact details: Veritas Privacy Office, privacy@veritas.com

Activities relevant to the data transferred under these Clauses: See section B below

Signature and date: ... As set out in the Agreement

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

The nature and purpose of the Processing, the types of Customer Personal Data that Veritas Processes and the categories of Data Subjects whose Personal Data is Processed is set out for each Service that Veritas provides, at www.veritas.com/privacy

- *Categories of data subjects whose personal data is transferred*

  Customer may submit Personal Data to the Services, the extent to which is determined and controlled by the exporter, and which may include but is not limited to the following categories of data subjects: Workers of the Data Exporter its Affiliates and the suppliers and customers, that are named as persons authorised to use the Services, and any other categories of individuals that correspond or interact with the Data Exporter in the course of its business.

- *Categories of personal data transferred*

  Customer may submit Personal Data to the Services, the extent to which is determined and controlled by the exporter, and which may include but is not limited to the following categories of Personal Data:

  First name Last name
  Contact information (company email/ phone, business address) IP address
  Miscellaneous categories of Personal Data that exist in the various communications and documents archived in the Service.

- *Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.*

  Customer may submit special categories of data to the Services, the extent to which is determined and controlled by the data exporter. In the context of the processing of the Customer Data in the Service: Miscellaneous categories of Sensitive Personal Data that exist in the various communications and documents archived in the Service.

- *The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).*

  Customer Personal Data will be transferred periodically throughout the term of the Agreement. Customer will have control over each transfer to Veritas.

- *Nature of the processing*

  Processing in support of performance of the Agreement, including provision of Services thereunder.

- *Purpose(s) of the data transfer and further processing*

  As necessary to perform the Services pursuant to the Agreement and as further specified in the Service privacy notice available at https://www.veritas.com/company/privacy.

- *The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period*

  Subject to Section 3 (e) and (f) of the DPA, for the duration of the Agreement, unless otherwise agreed upon in writing.

- *For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing*

  General authorisation for the engagement of sub-processor(s) from an agreed list available at https://www.veritas.com/content/dam/Veritas/docs/policies/sub-processors-for-veritas-service.pdf

C. COMPETENT SUPERVISORY AUTHORITY

Clause 13 shall apply as follows:

Where the data exporter is established in an EU Member State, the supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, shall act as competent supervisory authority; or

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679, the supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, shall act as competent supervisory authority; or

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679, The Data Protection Commission (DPC) shall act as competent supervisory authority; or

Where the data exporter is established in the United Kingdom or falls within the territorial scope of the application of UK Data Protection Legislation, the Information Commissioner's Office (ICO) shall act as competent supervisory authority.

Where the data exporter is established in the Switzerland or falls within the territorial scope of the application of Swiss Data Protection Legislation, the Data Protection and Information Commissioner's Office (FDPIC) shall act as competent supervisory authority.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Veritas maintains administrative, physical, and technical safeguards for the protection of the security, confidentiality and integrity of Customer Personal Data uploaded to the Services as described in this Annex II. Veritas will not materially decrease the overall security of the Services during the term of Agreement.

Veritas has implemented and maintains a security program that leverages a combination of the ISO/IEC 27001:2022-NIST 800-30, NIST 800-53R5, NIST CSF, BSIMM, DISA/CIS, CISA and other authoritative sources.

Veritas uses Microsoft Azure and/or Amazon Web Services as Sub-processors for purposes of providing the Services to Customer.

- For Technical and Organizational Measures applicable to Microsoft Azure (sub-processor) please refer to applicable terms and documentation here: https://www.microsoft.com/en-us/trust-center/privacy.
- For Technical and Organizational Measures applicable to Amazon Web Services (sub-processor) please refer to applicable terms and documentation here: https://aws.amazon.com/compliance/data-protection

Measures for Ensuring Physical Security of Locations at Which Personal Data are Processed

Web applications, communications, and database servers of Veritas are located in secure data centers. Veritas has implemented suitable measures in order to prevent unauthorized persons from gaining access to the data processing equipment. This is accomplished by:

- Establishing security areas;
- Securing the data processing equipment and personal computers;
- Establishing access authorizations for employees and third parties, including the respective documentation;
- Regulations/restrictions on card-keys;
- Restricting physical access to the servers by using electronically- locked doors and separate cages within facilities (e.g., production and development);
- Access to the data center is logged, monitored, and tracked via electronic and CCTV video surveillance by personnel; and
- Data centers are protected by security alarm systems, and other appropriate security measures, such as user-related authentication procedures, including biometric authentication in some instances, and/or electronic access cards.

Measures for Ensuring Ongoing Confidentiality, Integrity, Availability and Resilience of Processing Systems and Services

Veritas has implemented suitable measures to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services. This is accomplished by:

- Utilizing firewall, router, and VPN-based access controls to protect the private service networks and back-end-servers;
- Continuously monitoring infrastructure security;
- Regularly examining security risks by internal employees and third-party auditors;
- Role-based access control implemented in a manner consistent with principle of least privilege;
- Remote access to Veritas's network infrastructure is secured using various two-factor authentication tokens, or multi-factor authentication.
- Access to host servers, applications, databases, routers, switches, etc., is logged;
- Access and account management requests must be submitted through internal approval systems;
- Access must be approved by an appropriate approving authority. In most cases, the approval for a request requires two approvals at minimum: the employee's manager and the role approver or "owner" for the particular system or internal application;
- Passwords must adhere to the Veritas password policy, which includes minimum length requirements, enforcing complexity and set periodic resets;
- Password resets are handled via Veritas ticketing system. New or reset passwords are sent to the employee using internal secure, encrypted email system or by leaving a voicemail for the employee;
- Veritas's intrusion detection systems include signature-based network IDS, host-based IDS, and security incident and event

management (SIEM) systems. Veritas also uses commercial and custom tools to collect and examine its application and system logs for anomalies; and
- The SaaS Solution is developed leveraging solution architecture ensuring confidentiality, integrity, availability, and resilience.

Measures for User Identification and Authorization

Persons entitled to use the systems are only able to access data within the scope and to the extent covered by their respective access permission (authorization). This is accomplished by:

- Employee policies and training;
- Users have unique log in credentials – role-based access control systems are used to restrict access to particular functions;
- Monitoring activities;
- Effective and measured disciplinary actions;
- Controlling access in compliance with the security principle of "least privilege";
- Internal segmentation and logical isolation of Veritas's employees to enforce least privilege access policies;
- Regular review of accounts and privileges (typically every 12 months depending on the particular system and sensitivity of data it provides access to);
- Control of files, controlled and documented destruction of data; and policies controlling the retention of back-up copies

Measures for Ensuring the Ability to Restore the Availability and Access to Personal Data in a Timely Manner in the Event of a Physical or Technical Incident

Veritas has implemented suitable measures to ensure that data is protected from accidental destruction or loss. This is accomplished by:

- Veritas has implemented a Business Continuity and Disaster Recovery plan, which is subject to periodic testing;
- Global and redundant infrastructure that is set up with disaster recovery;
- Constantly evaluating data centers and Internet service providers (ISPs) to optimize performance for its customers in regard to bandwidth, latency and disaster recovery isolation;
- Situating data centers in secure co-location facilities that are ISP carrier neutral and provide physical security, redundant power, and infrastructure redundancy;
- Service level agreements from ISPs to ensure a high level of uptime;
- Timely failover capability; and
- Veritas maintains full capacity disaster recovery (DR) sites and tests its DR centers.

Measures of Pseudonymization and Encryption of Personal Data

Veritas has implemented suitable measures to prevent Personal Data from being read, copied, altered,

or deleted by unauthorized parties during the transmission thereof or during the transport of the data media. This is accomplished by:

- Use of adequate firewall and encryption technologies to protect the gateways and pipelines through which the data travels;
- Sensitive Personal Data is encrypted during transmission using up to date versions of TLS or other security protocols using strong encryption algorithms and keys;
- Protecting web-based access to account management interfaces by employees through encrypted TLS;
- End-to-end encryption of screen sharing for remote access, support, or real time communication; and
- Use of integrity checks to monitor the completeness and correctness of the transfer of data.
- SaaS offerings offer encryption at rest with customer unique encryption keys.
- Immutable write once rad many (WORM) storage is available in SaaS products where warranted.

Measures for Ensuring Data Quality

Veritas has implemented suitable measures to ensure that it is possible to check and establish whether and by whom Personal Data have been input into data processing systems or removed. This is accomplished by:

- An authorization policy for the input of Personal Data into memory, as well as for the reading, alteration, and deletion of such stored data;
- Authentication of the authorized personnel;
- Protective measures for Personal Data input into memory, as well as for the reading, alteration, and deletion of stored Personal Data, including by documenting or logging material changes to account data or account settings;
- Segregation and protection of all stored Personal Data via database schemas, logical access controls, and/or encryption;
- Utilization of user identification credentials;

- Physical security of data processing facilities; and
- Session time outs.

Measures for Ensuring Accountability

Veritas has implemented suitable measures to monitor, in accordance with applicable privacy laws, access restrictions of Veritas's system administrators and to ensure that they act in accordance with instructions received. This is accomplished by:

- Individual appointment of system administrators;
- Adoption of suitable measures to register system administrators' access logs to the infrastructure and keep them secure, accurate and unmodified for a reasonable period of time;
- Regular audits of system administrators' activity to assess compliance with assigned tasks, the instructions received by Controller and applicable laws; and
- Keeping an updated list with system administrators' identification details (e.g., name, surname, function, or organizational area) and responsibilities.

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing

Veritas has implemented annual testing of the SaaS Solution and relevant processes including security incident response tests, Business Continuity and Disaster Recovery tests, Penetration testing.

Measures for certification/assurance of processes and products shall be requested under a non-disclosure agreement or confidentiality clause

ANNEX III

LIST OF SUB-PROCESSORS

General authorisation for the engagement of sub-processor(s) from an agreed list available at:

https://www.veritas.com/content/dam/Veritas/docs/policies/sub-processors-for-veritas-service.pdf