Data Processing Addendum

This Data Processing Addendum ("DPA") between Tenable and Customer is incorporated into and made part of the Master Agreement (the "Agreement") between Customer and Tenable. Capitalized terms used but not defined in this DPA have the meanings given to them in the Agreement.

(1) Definitions.

(a) "Data Controller" means the Party which determines the purposes and means of the Processing of Personal Data.

(b) "Data Processor" means the Party which Processes the Personal Data on behalf of the Controller. A "Sub-Processor" means any third party who performs Processing for the Data Processor.

(c) "Data Subject" means an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

(d) "GDPR" means the General Data Protection Regulation, which is the European Union's ("EU") Regulation 2016/679 the regulates the processing of Personal Data and takes effect May 25, 2018.

(e) "Personal Data" as used in this Addendum have the meanings given in the GDPR.

(f) "Processing" means any operation or set of operations which is performed on Personal Data, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, erasure or destruction.

(g) "Supervising Authority" means an independent public authority which is established by a Member State of the EU pursuant to Article 51 of the GDPR and has appropriate jurisdiction over Tenable with regards to Tenable's Processing of Personal Data pursuant to this DPA.

(2) Purpose. In the course of providing the Products to you in accordance with the Agreement, Tenable shall have a legitimate interest in Processing Scan Data on your behalf. Customer Data may include Personal Data. The purpose of this DPA is to document the agreement between the Parties relating to the possible Processing of Personal Data in accordance with the requirements of the GDPR. This DPA will control in the event of any conflict with the Agreement. This DPA will take effect on the date of Customer's initial purchase of an applicable Product which may cause Tenable to Process Personal Data on behalf of Customer and will remain in effect until, and automatically expire upon, the date on which Tenable ceases to Process Personal Data on behalf of Customer.

(3) Roles Generally. The Parties agree and acknowledge that if there is any Personal Data within the Scan Data then as between the Parties: (i) Customer is the Data Controller; and (ii) Tenable shall act as Data Processor acting on behalf of and at the direction of the Data Controller.

(a) Customer as Data Controller. As Data Controller, the Customer has sole control over the: (i) process of obtaining Personal Data from Data Subjects and all necessary consents for such Personal Data; (ii) categories of Data Subjects and Personal Data to be Processed; and (iii) accuracy, quality, and legality of the Personal Data and the means by which it was acquired.

(b) Tenable as Data Processor. As Data Processor, Tenable shall Process the Personal Data in accordance with the following: (A) the Agreement and any transaction documents thereunder; and (B) reasonable instruction provided by Customer to Tenable which is otherwise consistent with the Agreement, including all instructions provided via email. Tenable will not Process Customer Data for any other purpose than as instructed by Customer and as contemplated under the Agreement.

(4) Data Subjects.

(a) Consent. The control of Personal Data remains with Customer, and as between Customer and Tenable, Customer shall remain the Data Controller at all times for the purposes of the Agreement and this DPA. Customer is solely responsible for compliance with its obligations as Data Controller under all applicable data protection laws, in particular for justification of any transmission of Personal Data to Tenable (including providing any required notices and obtaining any required consents, or establishing an alternative justification for legally collecting Personal Data for Processing). For the avoidance of doubt, Tenable has no way of determining or knowing what information will be Scanned so the parties agree that Customer remains solely responsible for its decisions and actions concerning the Processing and use of the Personal Data.

(b) Requests. The GDPR grants Data Subjects the right to obtain from the Controller confirmation as to whether or not the Data Subject's Personal Data is being processed, and if so, Data Subjects have the right to access the Personal Data and other relevant information. As a Data Processor, Tenable will not respond to requests made directly to Tenable by a Data Subject for access to, correction of, or deletion of such Data Subject's Personal Data. Data Controller shall be solely responsible for such obligations with regards to the Data Subjects whose data resides on Customer's networks. Tenable shall not respond directly to any such request made by a Data Subject except to confirm that any such request relates to Customer.

(b) Rectification and Erasure. The GDPR requires Data Controllers to properly rectify or erase Personal Data upon reasonable request of the Data Subject. Tenable's Products have or will have features which enable the Customer to erase or rectify any Personal Data which may exist in the Scan Data. If the Customer is unable to do so on their own (or requires assistance), Customer may provide written request with instructions to Tenable to perform such deletions or rectifications on Customer's behalf. To the extent such request and instructions are technically feasible and legally permissible, Tenable shall (for a fee to Customer) carry out such request and instructions at the sole cost of Customer. Tenable shall only accept such requests from an authorized Customer administrator.

(c) Assistance to Controller. As Data Processor, Tenable shall provide reasonable assistance to Customer (at Customer's sole cost and expense) in response to Customer's written request for assistance in relation to: (i) a request, complaint, notice, or communication relating to Tenable's Processing of Customer Data received from a Data Subject whose Personal Data is contained within the Scan Data; (ii) any investigation, request or notice from a Supervising Authority; (iii) a privacy impact assessment conducted by Customer which is relevant to Customer's Processing of Personal Data in accordance with the Agreement or a transaction conducted thereunder; or (iv) a Customer's request (not to be made more than once per year unless requested by a Supervisory Authority) for Tenable to provide a written attestation that Tenable is in material

compliance with thisDPA.

(5) Lawfulness of Processing. Customer and Tenable agree that the Processing of Personal Data under this Addendum by Tenable is carried out in accordance with Article 6 of the GDPR (*Lawfulness of Processing*). In particular, such Processing by Tenable is necessary for the purposes of the legitimate interests pursued by the Customer and Tenable.

(6) Tenable's Personnel. "Tenable's Personnel" means Tenable's personnel who are engaged in Processing of Personal Data pursuant to this DPA. Tenable shall thoroughly inform all Tenable Personnel of their obligations of confidentiality under the Agreement, this DPA and the GDPR. Furthermore, Tenable shall provide detailed training to all Tenable Personnel on the confidential nature of Personal Data. Such trainings shall include explanation of their duties and responsibilities. Finally, Tenable shall be responsible for entering into written non-disclosure agreements with Tenable Personnel who have obligations of confidentiality intended to survive the termination of employment of Tenable Personnel. Access to Customer's Scan Data, if any, is limited to Tenable's Personnel who require such access for the purpose of Processing Customer Data on behalf of Customer.

(7) Sub-processors. Customer expressly authorizes Tenable to utilize Sub-Processors in furtherance of Tenable's duties as a Processor. Tenable shall execute separate written agreements with each Sub-Processor that contain obligations similar to those set forth in this DPA. Tenable shall be responsible for each Sub-Processor's compliance with this DPA. Customer's sole and exclusive remedy to any objection to Tenable's use of a Data Sub-Processor shall be for Customer to delete its Scan Data from the Product. A current list of Tenable's Sub-Processors may be found at https://www.tenable.com/gdpr-alignment (or successor location). For the avoidance of doubt, no refund or relief from any payment obligation shall be available to Customer based on Tenable's choice of Sub-Processor.

(8) Security Incident. In the event that Tenable becomes aware of or reasonably believes there has been an unauthorized, unlawful or wrongful disclosure of, or access to Personal Data that Tenable is Processing on behalf of Customer (a "Security Incident"), Tenable shall (to the extent known and permitted under law) provide Customer with prompt notice of such Security Incident. Such notice shall include details of the Security Incident, steps taken to mitigate the potential risks, and reasonable steps Tenable recommends Customer take to address the Security Incident. The Parties shall cooperate in good faith to help limit the effects of such Security Incident and prevent a recurrence. Customer, as Data Controller, shall be solely responsible for providing notifications to the Supervising Authority and/or any Data Subjects; provided, however, Tenable shall provide Customer with reasonable assistance and cooperation in carrying out such notifications. Tenable's notification of or response to a Security Incident under this Section 8 will not be construed as an acknowledgement by Tenable of any fault or liability with respect to the Security Incident.

(9) Security of Processing. Tenable shall implement and maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk associated with Processing. Specifically, Tenable shall maintain appropriate safeguards to protect Customer Data from unauthorized or unlawful Processing or a Data Breach.

(10) Data Impact Assessments; Record Keeping. Tenable, as Data Processor shall conduct Data Impact Assessments as necessary and shall maintain appropriate records of all Data Processing Activities.

(11) Transfer of Personal Data to Third Countries. Tenable is certified under the EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield frameworks. Tenable shall maintain and comply with such certifications during the Term of the Agreement. These frameworks provide Tenable a means to comply with data requirements when transferring Personal Data from the EU or Switzerland to the United States.

(12) Audit Rights. Except to the extent required by the GDPR, Customer may audit Tenable's compliance with its obligations under this Addendum up to once per year. Tenable will contribute to such audits by providing Customer or Customer's Supervisory Authority with the information and assistance reasonably necessary to conduct the audit, including any relevant records of Processing activities applicable to the Services. To request an audit, Customer must submit a detailed proposed audit plan to Tenable at least two weeks in advance of the proposed audit date. Tenable will review the proposed audit plan and provide Customer with any concerns or questions. Tenable will work cooperatively with Customer to agree on a final audit plan. Nothing in this section shall require Tenable to breach any duties of confidentiality. The audit must be conducted during regular business hours at the applicable facility, subject to the agreed final audit plan and Tenable's health and safety or other relevant policies, and may not unreasonably interfere with Tenable business activities. If the requested audit scope is addressed in an SSAE 16/ISAE 3402 Type 2, SOC 1 or SOC 2, ISO, NIST or similar audit report performed by a qualified third party auditor ("Audit Reports") within twelve (12) months of Customer's audit request and Tenable confirms there are no known material changes in the controls audited, Customer agrees to accept those findings in lieu of requesting an audit of the controls covered by the report.

(13) Analytics. Customer acknowledges and agrees that Tenable may create and derive from Processing related to the Products anonymized and/or aggregated data that does not identify Customer or any natural person, and use, publicize or share with third parties such data to improve Tenable's products and services and for its other legitimate business purposes.

(14) Data Retention Policy. Tenable shall implement and maintain an appropriate data retention policy which stores backups of Scan Data and which takes into account technical and legal requirements to ensure a retention period appropriate to the risk associated with Processing.

(15) Data Protection Officers. Tenable's initial Data Protection Officer is Stephen A. Riddick (General Counsel). Customer is responsible for providing notice to Tenable of Customer's Data Protection Officer. Both parties are responsible for keeping the other party informed of any changes to their respective Data Protection Officers.