

NETWORK SERVICE SCHEDULE

INTERNET2 VOLUMETRIC DDoS MITIGATION SERVICE

This Internet2 Volumetric DDoS Service Schedule (“**Network Service Schedule**” or “**Subscriber Agreement**”) is entered into and made effective as of March 9, 2020 (the “**Service Schedule Effective Date**”), between University Corporation for Advanced Internet Development d/b/a Internet2 (“**Internet2**”) and Virginia Polytechnic Institute and State University (“**NSP**” or “**Subscriber**”) (Internet2 and NSP are each referred to herein as a “**Party**,” and collectively “**Parties**”) and applies only where NSP orders the Network Service from Internet2 pursuant to one or more Network Service Orders. This Network Service Schedule is incorporated by reference into, and is subject to, the Master Service Agreement (the “**MSA**”) entered into between the Parties on February 1, 2014.

Prior to the Service Schedule Effective Date, Internet2 and Radware, Inc. (“**Provider**” or “**Radware**”) executed the Master Service Agreement for DDoS Service (“**Internet2 Radware Agreement**”) pursuant to which, Radware: (1) granted Internet2 certain rights to resell the Network Service to NSP and (2) agreed to be bound by all of the terms and conditions of the Radware Terms of Service.

The Parties agree as follows:

1. Certain Rights; Obligations; Restrictions

1.1 **Use of the Network Service by NSP.** Subject to all the terms and conditions of this Network Service Schedule and the Radware Terms of Service (for purposes of the Radware Terms of Service, NSP is referred to as “**Subscriber**” and collectively with Tenants as “**Customer**”), Internet2 grants NSP a nonexclusive, enterprise-wide, fully paid-up worldwide right and license for the duration of the Service Term to access and use, and permit and enable Authorized NSP Users to access and use, the Network Services. The Network Services are being provided by Radware and not by Internet2. For the avoidance of doubt, NSP agrees that except with respect to communicating (a) modifications to the Network Services, (b) suspension or termination of the Network Services, and (c) Service Level Agreement service credits to NSP, and providing refunds to NSP pursuant to Section 9.12 of the Radware Terms of Service, the Radware Terms of Service create no obligations for Internet2 and is not binding on Internet2 in any way. NSP’s sole remedy, except as provided for in Section 5.1, related to the provision of Network Services shall be against Radware and not Internet2.

1.2 Resale of Network Services by NSP.

- a. Subject to the terms and conditions of this Network Service Schedule and the Radware Terms of Service, Internet2 grants NSP:
 - i. the right to, but not the obligation to, market the Network Services to Qualified Persons throughout the Term of this Network Service Schedule; and
 - ii. the right to, but not the obligation to, enter into an unlimited number of Tenant Customer Agreements with any of (and only with) NSP’s downstream customers who are Qualified Persons (each of whom then become “**Tenants**”) once they purchase the Tenant Services from NSP in connection with this Network Service Schedule and Radware accepts the related Service Order) for the provision of Tenant Services, which shall permit and enable Tenants to access and use, and permit and enable Authorized Tenant Users to access and use, the Network Services.
- b. NSP shall not permit any Tenant to market or resell the Tenant Services. Further, NSP shall ensure each Tenant waives all rights to bring and does not bring any Claims against Internet2 related to the Tenant Services.
- c. Radware Terms of Service.
 - i. NSP shall not (a) resell the Network Services to Tenants without entering into a Tenant Customer Agreement that includes, as a binding exhibit incorporated into the body of such agreement, the Radware Terms of Service and a Service Term, or (b) make any representations, warranties, or covenants (express or implied) regarding the Network Services to any Tenants.
 - ii NSP shall acknowledge, and require all Tenants to acknowledge, the Radware Terms of Service by

signing the Radware Terms of Service Acknowledgement. NSP shall provide a copy of the Radware Terms of Service Acknowledgement to Internet2 and Internet2 will provide a copy of such acknowledged Radware Terms of Service to Radware.

- d. **Non-Exclusivity.** NSP acknowledges that its right to resell Network Services under this Network Service Schedule is non-exclusive. Except as expressly set forth, nothing in this Network Service Schedule shall limit in any manner Internet2's marketing, distribution or sales activities or its rights to market, distribute or sell, directly or indirectly, or appoint any other person or company as a reseller, licensee or agent for the Network Services.

1.3 Orders for Network Services

- a. For purposes of this Network Service Schedule, Section 2.1(a) of the MSA does not apply. NSP may request Network Services for itself or a Tenant by submitting a Network Service Order to Internet2. NSP acknowledges and agrees that NSP is solely responsible for the accuracy of all Network Service Orders and other information that it provides to Internet2 and that for any such Network Service Order for a Tenant, NSP must clearly indicate that the Network Service is being ordered is for a Tenant and provide all required Tenant details. Upon receiving a Network Service Order from NSP, Internet2 shall submit a related Service Order to Radware for review and acceptance. If Radware accepts a Service Order related to a Network Service Order, Internet2 shall notify NSP of the acceptance and anticipated Service Start Date provided by Radware.
- b. In addition to Section 2.1(b) of the MSA, each accepted Network Service Order shall be subject to the terms and conditions of the Radware Terms of Service.
- c. For purposes of this Network Service Schedule, Section 2.1(c) of the MSA does not apply. The Network Services shall be made available to the NSP or a Tenant on the Service Start Date which shall be the earlier of (x) the date of the onboarding of NSP or a Tenant by Radware, as evidenced from a successful diversion test or (y) within thirty (30) days of the anticipated Service Start Date provided by Radware unless Radware causes such delay beyond the thirty (30) days. For clarity purposes, in the event NSP or Tenant causes the delayed onboarding beyond the thirty (30) days, NSP shall be responsible for payment of all fees starting on such Service Start Date, notwithstanding the fact that the Network Service may not yet be available.
- d. In the event NSP has more than five (5) Sub-Tenants on its network, NSP must purchase a Sub-Tenant Five Pack. Each additional Sub-Tenant Five Pack covers up to an additional five (5) Sub-Tenants. If NSP has more than twenty-five (25) Sub-Tenants, Internet2 and NSP will work together in good faith to negotiate a custom solution.

2. Term

2.1 **Term.** The term of this Network Service Schedule shall commence as of the Service Schedule Effective Date and remain in effect for three (3) years (the "Initial Term"), unless earlier terminated in accordance with a Party's rights hereunder or by mutual written agreement of the Parties. This Network Service Schedule may be renewed upon mutual written agreement of the Parties (each a "Renewal Term"). The Initial Term and any Renewal Term are collectively referred to herein as the "Term."

2.2 **Network Service Order Term.** For purposes of this Network Service Schedule, Section 3.2 of the MSA does not apply. The term of each Network Service Order shall commence on the Service Start Date and continue for the Service Term noted therein.

3. Pricing and Payment Term

3.1 **Pricing.** The rates for the Network Services are set forth in Exhibit A.

3.2 **Commencement of Billing.** For purposes of this Network Service Schedule, the term "Network Service Date" used under Section 4.2 of the MSA shall be deleted and replaced with "Service Start Date."

3.3 **Payment of Invoices.** For purposes of this Network Service Schedule, Section 4.3(b) of the MSA shall not apply. Internet2 may increase the rates in Exhibit A when the rates for the Network Service is increased by Radware pursuant to the terms of the Internet2 Radware Agreement and shall only apply to new Network Service Orders submitted after the effective date of the applicable rate increase under the Internet2 Radware Agreement.

3.4 **Service Overage.** In the event actual usage of any Network Service ordered by NSP, for itself or a Tenant, exceeds the level ordered by NSP or exceeds any Network Service limitation(s), such as, but not limited to, limitations on traffic level (legitimate or attack, as applicable), the number of diversions, duration of diversions, number of protected assets or any other limitation (each an "**Overage**"), Internet2 will inform NSP about the Overage and in such event NSP will either buy an upgrade and/or an add-on covering the Overage at an additional Fee (an "**Overage Fee**") and/or stop, or cause the applicable Tenant to stop, the Overage immediately. If NSP is required to pay an Overage Fee but does not do so, Internet2 will not pay Radware any related Overage Fees and NSP or Tenant's applicable Network Service may be suspended or terminated without NSP being entitled to any remedies, refund, or any other form of compensation. A suspension or termination of the Network Service as noted above, shall not absolve NSP of its payment obligations for the entire Service Term.

4. Indemnification

4.1 NSP agrees to defend, indemnify, and hold harmless Internet2 and each of its Indemnitees from and against all Damages, incurred in connection with any third party (including Radware) Claims (i) resulting from NSP's failure to abide by the Radware Terms of Service; (ii) resulting from NSP's failure to include the Radware Terms of Service in any Tenant Customer Agreement; (iii) arising from or in connection with any Tenant Customer Agreement, including from any representations, warranties, covenants, or licenses made by NSP to a Tenant in excess of this Network Service Schedule, the Radware Terms of Service, or the Service Level Agreement to the extent allowable by Virginia law. Nothing herein shall be construed as an express or implied waiver of NSP's sovereign immunity.

5. Limitation of Liability.

5.1 Notwithstanding any provision of the MSA, including, for the avoidance of doubt, Section 8.5, for purposes of this Network Service Schedule, Section 8.2 of the MSA shall not apply and the following shall apply:

NOTWITHSTANDING ANY CONTRARY PROVISION SET FORTH IN THIS NETWORK SERVICE SCHEDULE, THE PARTIES EXPRESSLY AGREE THAT IN NO EVENT SHALL EITHER PARTY'S ENTIRE LIABILITY FOR ANY LIABILITIES, LOSSES, CLAIMS, JUDGMENTS, DAMAGES, EXPENSES OR COSTS (INCLUDING REASONABLE FEES AND EXPENSES OF COUNSEL) ARISING OUT OF THIS NETWORK SERVICE SCHEDULE, WHETHER IN CONTRACT, TORT OR OTHERWISE, EXCEED FIFTY THOUSAND DOLLARS (\$50,000). THE FOREGOING CAP ON LIABILITY SHALL, HOWEVER, NOT BE APPLICABLE TO A PARTY'S INDEMNITY OBLIGATION UNDER THE MSA AND THIS NETWORK SERVICE SCHEDULE.

6. Warranties; Disclaimers; Additional MSA Changes

6.1 NOTWITHSTANDING ANY PROVISION OF THE MSA, INCLUDING, FOR THE AVOIDANCE OF DOUBT, SECTION 9.4, FOR PURPOSES OF THIS NETWORK SERVICE SCHEDULE, INTERNET2 MAKES NO (AND HEREBY DISCLAIMS ALL) WARRANTIES, REPRESENTATIONS OR CONDITIONS, WHETHER WRITTEN, ORAL, EXPRESS, IMPLIED OR STATUTORY, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, TITLE, NONINFRINGEMENT, OR FITNESS FOR A PARTICULAR PURPOSE, WITH RESPECT TO THE USE, MISUSE, OR INABILITY TO USE THE NETWORK SERVICE (IN WHOLE OR IN PART).

6.2 **Third Party Applications.** Internet2 does not endorse, and is not responsible or liable for, the services or features provided by any Third Party Application that NSP might install or utilize in connection with the Network Service. NSP acknowledges and agrees that Internet2 shall not be responsible or liable, directly or indirectly, for any damage or loss caused or alleged to be caused by or in connection with use of or reliance on any Third Party Applications.

6.3 Except as otherwise provided for in Section 5.1 of this Network Service Schedule, under no circumstances shall Internet2 be liable to NSP for the Network Service or for the acts or omissions of Radware or any other Person using the Network Service.

6.4 In addition to the Modification Notice provided for in Section 5.6 of the MSA, Internet2 shall provide NSP notice of any modification to the Network Service made by Radware pursuant to Section 3.3 of the Radware Terms of Service, if Radware provides Internet2 such notice of modification.

7. Termination of Network Service Schedule

7.1 In addition to the termination provisions under Section 12.1 and 12.4 of the MSA, termination of the Internet2 Radware Agreement shall result in the automatic termination of this Network Service Schedule and all exhibits attached hereto, Network Service Orders under this Network Service Schedule and all Radware Terms of Service.

7.2 For purposes of this Network Service Schedule, Section 12.3 of the MSA shall not apply.

7.3 If NSP (or Tenant when applicable) terminates this Network Service Schedule, or related Network Service Order, Service Term and/or Radware Terms of Service as provided for under Section 3.3, 5.1(d) or 8.6 of the Radware Terms of Service, Internet2 shall be responsible for refunding any pre-paid fees paid by NSP or Tenant only to the extent that Radware refunds such fees to Internet2. In the event Tenant is owed a refund under this Section, Internet2 shall pay such refund to Subscriber and Subscriber shall be responsible for providing such monies to Tenant. In the event NSP (or Tenant when applicable) terminates this Network Service Schedule, or related Network Service Order, Service Term and/or Radware Terms of Service other than as provided for under Section 3.3, 5.1(d) or 8.6 of the Radware Terms of Service, NSP and Tenant are not entitled to and will not be refunded any pre-paid fees related to any such Network Service Schedule, Network Service Order, Service Term and/or Radware Terms of Service.

8. Service Level Agreement and Support Services

8.1 Notwithstanding anything in the MSA to the contrary, for the purpose of this Network Service Schedule and the Network Services ordered hereunder, Internet2 is in no way required to provide any support services to NSP or any Tenant. Any support services related to the Network Services are included in the Service Level Agreement provided by Radware under the Radware Terms of Service.

8.2 For purposes of claims for service credit for NSP's use of the Network Services under the Service Level Agreement, NSP shall be responsible for submitting all claims to Internet2, who will submit such claims to Radware; Radware shall be responsible for validating any such claims. Service credits will be in the form of additional service days at the end of the Service Term.

8.3 For purposes of claims for service credit for Tenant's use of the Network Services under the Service Level Agreement, NSP or Tenant shall be responsible for submitting all claims to Internet2, and Radware shall be responsible for validating any such claims. Service credits will be in the form of additional service days at the end of the Service Term.

9. Certain Definitions

Any capitalized terms used herein shall have the meaning set forth in the MSA unless otherwise defined herein. The following capitalized terms shall have the meaning set forth below:

"Authorized NSP User(s)" means NSP's employees or Contractor/Agents who are authorized to access the Network Services on behalf of NSP. For the avoidance of doubt, Authorized Tenant Users are not Authorized NSP Users.

"Authorized Tenant User(s)" means Tenant's employees or Contractor/Agents who are authorized to access the Network Services on behalf of Tenant. For the avoidance of doubt, Authorized Tenant Users are not Authorized NSP Users.

"Claim(s)" means, individually and collectively, claims, actions, demands, suits, or proceedings.

“Damages” means, individually and collectively, damages, costs, liabilities, and losses and expenses, including reasonable attorneys’ fees.

“Indemnitees” means, collectively, Internet2, its successors, assigns, Affiliates and subsidiaries and each of their respective members, managers, directors, officers, shareholders, agents, employees and representatives.

“Internet2 Research and Education Network Member” means a U.S.-based non-profit or not-for-profit organization that is substate, state or multistate in scope and that has a principal mission to provide network infrastructure and services primarily to the research and education community in the relevant geographic area, including, but not limited to, access to the national Internet2 Network infrastructure and services.

“Network Service” or “Service” means, for the purposes of this Network Service Schedule, the services provided by Radware under the Radware Terms of Service. For purposes of NSP, the Services shall include one Sub-Tenant Five Pack at no additional fee. In the event NSP has more than five (5) Sub-Tenants on its network, NSP will need to purchase additional Sub-Tenant Five-Pack(s).

“Network Service Order” means, for the purposes of this Network Service Schedule, an order form that is used by NSP to contract for Network Services (either for itself or for Tenants), and which is executed by NSP. Each such accepted Network Service Order will be incorporated by reference into this Agreement. A current version of the Network Service Order is set forth in Exhibit C.

“Qualified Person(s)” means (a) a higher education member of Internet2, (b) an Internet2 Research and Education Network Member, (c) a K-12 educational institution, higher education institution, library, museum, or other not-for-profit organization that in Internet2’s reasonable judgment has or facilitates a research or educational mission, or (d) other institutions as agreed to in writing by Internet2 and Radware.

“Radware Terms of Service” means the modified Radware Terms of Service attached hereto as Exhibit B.

“Radware Terms of Service Acknowledgement” means a signed copy of Exhibit B, as signed by the Subscriber or Tenant as applicable.

“Service Level Agreement” means the Radware Service Level Agreement attached to the Radware Terms of Service as Attachment 2 that sets forth the support services and level of service provided of Radware for the Network Services.

“Service Order” means an order form that is used by Internet2 to contract for Network Service on behalf of the NSP with Radware.

“Service Start Date” means, for each Network Service, the date of the onboarding of a Subscriber or a Tenant, as evidenced from a successful diversion test or within thirty (30) days of the anticipated Service Start Date provided by Radware after reviewing the requested Service Start Date in the Service Order, whichever is earlier, unless such delay beyond the thirty (30) days is caused by the Radware.

“Service Term” means the fixed term designated in a Network Service Order, which may be terminated solely in accordance with the Radware Terms of Service.

“Sub-Tenant” means any Person that is on a Subscriber’s network, has its own publicly registered Autonomous System Number (“ASN”), and does not choose the option to become a Tenant. Under no circumstances shall K-12 schools and libraries that are eligible to receive the FCC’s Universal Service Funds, regardless of whether they have an ASN, be considered a Sub-Tenant and Subscriber will not be required to pay a Sub-Tenant Usage Fee for any such entity. Except as otherwise determined by Internet2 in its sole discretion, any Person that is an Internet2 Research and Education Network Member is not eligible to be a Sub-Tenant and can receive Services only by becoming a Subscriber.

“Sub-Tenant Five-Pack” means the vehicle through which a Subscriber’s Sub-Tenant is covered under the Services.

“Sub-Tenant Usage Fee” means a fee payable by a Subscriber with more than five (5) Sub-Tenants.

“Tenant” means any Qualified Person to whom NSP resells the Network Services, as contemplated in, and consistent with, the terms of this Network Service Schedule. Tenant does not include a protected network of NSP that does not purchase Tenant Services from NSP. Tenant does not include downstream customers or Sub-Tenants of NSP who do not purchase Tenant Services from NSP. Except as otherwise determined by Internet2 in its sole discretion, any Person that is an Internet2 Research and Education Network Member is not eligible to be a Tenant and can receive Services only by becoming a Subscriber.

“Tenant Customer Agreement” means an agreement under which a NSP resells the Network Services as Tenant Services to a Tenant as contemplated by, and consistent with the terms of, this Network Service Schedule and which must include as a binding exhibit the Radware Terms of Service.

“Tenant Services” means the Network Services that NSP resells to a Tenant.

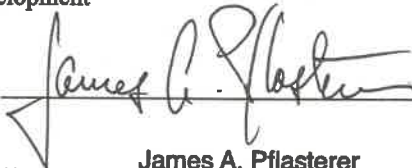
“Third Party Applications” means any Third Party software or application.
The Parties have executed this Network Service Schedule as of the Service Schedule Effective Date.

ACCEPTED AND AGREED:

NSP

University Corporation for Advanced Internet
Development

DocuSigned by:
By: Patricia K. Branscome
49FF509E7C9243B...

By: 
Name: James A. Pflasterer

Name: Patricia K. Branscome

Title: Director, IT Procurement & Licensing Solutions

Title: CFO

Exhibit A

Pricing

NSP/Subscriber Pricing

The following pricing shall apply for all orders of Network Services for use by NSP

Service	Service Detail	MRC	NRC
Internet2 Volumetric DDoS Mitigation Service	Set Up and OnBoarding for NSP/Subscriber	N/A	\$2000.00
Internet2 Volumetric DDoS Mitigation Service	Monthly Clean Traffic Includes: 1 Gbps of Monthly Clean Traffic Use of the Portal Access to SoC Direct Connect	\$6,000.00	N/A
Sub-Tenant Five Pack	Up to five (5) additional Sub-Tenants per Five Pack	\$500.00	N/A

Tenant Pricing

The following pricing shall apply for all orders of Network Services for use by Tenant

Service	Service Detail	MRC	NRC
Internet2 Volumetric DDoS Mitigation Service	Set Up and OnBoarding for Tenant	N/A	\$1000.00
Internet2 Volumetric DDoS Mitigation Service	Monthly Clean Traffic Includes: Monthly Clean Traffic (at level determined by NSP, but in no instance more than what NSP has ordered) Use of the Portal Access to SoC Direct Connect	\$500.00	N/A

Additional Pricing

Additional fees will apply if NSP or Tenant requires emergency onboarding due to a DDOS Attack.

Exhibit B

Radware Terms of Service

Provider's commitments to the Customer are as provided in these Terms of Service. Internet2 alone will be solely responsible for any commitments it makes to any Customers that are exceeding or in conflict with these Terms of Service and Provider will have no responsibility for fulfilling said commitments.

1 RELATIONSHIP STRUCTURE

1.1 Third Party Beneficiaries.

(a) **Provider.** Provider will be deemed a third-party beneficiary of these Terms of Service with respect to Customer and as such has the right to (i) enforce these Terms of Service directly against Customer to the extent that Provider is harmed by Customer's breach of these Terms of Service and (ii) defend against claims brought by Customer under these Terms of Service or under any other theory of liability and in so defending utilize, among others, any limitations and protections afforded by these Terms of Service, including any limitations of liability included herein.

(b) **Subscriber.** Subscriber will be deemed a third-party beneficiary to Section 2.2(b) of the FA that provides that (i) Provider will be bound by the terms and conditions in these Terms of Service, and (ii) each Subscriber is a third-party beneficiary of Section 2.2(b) of the FA as to Provider and has the right to enforce these Terms of Service directly against Provider. Accordingly, by way of example only, where these Terms of Service create an express indemnification obligation of Provider, a Customer Indemnitee will have the right to enforce such indemnification obligation against Provider directly as a third party beneficiary of Section 2.2(b) of the FA.

2 CUSTOMER'S USE OF THE SERVICES

2.1 Except as authorized in these Terms of Service, Customer will not: (a) authorize any Person to access and/or use the Services other than Customer's Authorized Users; (b) rent, lease, loan, export or sell access to the Services to any third party except Customer's Authorized Users; or (c) Abuse the Service. For purposes of clarification, and notwithstanding the foregoing, this Section 2.1 shall not be deemed to prevent Customer from reselling the Services to Tenants if Customer is a Subscriber.

2.2 If Customer is a Subscriber, Customer agrees that it will not resell the Service to any Tenant without first entering into with the Tenant a Tenant Customer Agreement which includes as an exhibit, incorporated into the body of such agreement, a copy of these Provider Terms of Service. Further, Customer agrees that it will make no representation, warranty, or covenant (whether express or implied) regarding the Services in any way. Notwithstanding anything to the contrary, Provider makes no representation, warranty, or covenant and shall have no liability whatsoever to Subscriber in its capacity as a reseller of the Services to Tenants. Provider makes no representation, warranty, or covenant and shall have no liability whatsoever to any Tenant and no Tenant shall be deemed a third-party beneficiary of these Terms of Service nor of any Agreement between Provider and Internet2.

2.3 Customer agrees to (i) follow traffic redirection actions in accordance with the Traffic Redirection Command Policy and (ii) disclose to Provider all information necessary so as to enable Provider to configure the Service, including Customer IP addresses subscribed to the Service (which such addresses must be tied to a valid ORG ID in the appropriate registry (ARIN, RIPE, APNIC, LACNIC, AFRINIC, etc.)). Customer will further notify Provider in writing about any new Protected Assets and/or any changes in any Protected Assets that may affect the Service.

2.4 Provider will ensure that all servers that will transmit or process Customer's traffic are located only in datacenters located in the continental United States and will not send any traffic originating in the United States to Scrubbing Centers located outside of the United States. Customer acknowledges, agrees and consents that in order

to make the Service continuously available for the Customer and in order for Provider to maintain the Service Levels provided for in the SLA, Provider may need to transmit the traffic directed to the Customer's Protected Assets originating from locations outside of the United States, to Scrubbing Centers located outside of the United States. Customer agrees that Provider may do so in its sole discretion, without first notifying Customer of any such transmission and without having to obtain the Customer's or any third party's separate and specific consent for any such transmission.

2.5 Customer further acknowledges and agrees that, when applicable, Customer is the Data Controller of the Customer's Personal Information and as such Customer will comply with its obligations as Data Controller under the Privacy & Data Security Laws, including, without limitation, providing any required notices and obtaining any required consents. Customer further acknowledges and agrees that Provider is the Processor of the Customer's Personal Information that is successfully diverted to Provider's Scrubbing Centers and authorizes Provider to engage other Processors for carrying out processing activities on behalf of the Customer.

2.6 Notwithstanding anything in these Terms of Service to the contrary, Customer will have the right to develop Customer Applications, and in connection therewith (and at no charge) Provider will provide the format of the interfaces or protocols provided under these Terms of Service, if any, for the API to the extent necessary for the Customer to develop any Customer Applications. Customer will have the right to use all Customer Applications and to distribute such Customer Applications to Authorized Users and to any other Persons to whom Provider has made the API available, for use by such Persons and their respective users. As between any Customer and Provider, the Customer will own all rights, title and interest, including all Proprietary Rights, in and to all Customer Applications.

3 PROVIDER'S DELIVERY OF SERVICE

3.1 Provider agrees to supply the Service in accordance with the terms of these Terms of Service and the SLA.

3.2 Provider acknowledges and agrees that, when applicable, Provider is the Data Processor of the Customer's Personal Information that is successfully diverted to Provider's Scrubbing Centers and as such Provider will comply with its obligations as Data Processor under the Privacy & Data Security Laws and, where applicable, pursuant to Provider's Data Protection Code of Conduct.

3.3 Modification. Provider reserves the right to modify the Services at any time, upon prompt written notice to Internet2 of any such modification (who will in turn notify Customer). If Provider makes any modification that materially and adversely affects Customer, Customer will have the right to terminate these Terms of Service and any related Service Order and Service Term on thirty (30) days' notice to Provider and Internet2, provided that Provider has not reversed such modification in such thirty (30) day period. Such notice of termination must be provided within thirty (30) days after Customer receives written notice from Internet2 of any such modification.

3.4 Emergency Action. The Parties agree that if Provider, in its sole discretion, determines that an emergency action is necessary to protect its own network, Provider may temporarily block any path over its network used by Customer.

4 DATA

4.1 Rights in and to Data.

(a) **Service Data.** Provider shall have the right to use, reproduce, modify, and otherwise exploit Service Data for the purpose of improving and enhancing the Service, monitoring the performance of the Service, and performing internal research and development of other products and services of Provider. In any event that Provider distributes Service Data or derivative works incorporating Service Data, to any third party, such distribution shall not directly identify Customer and/or its Authorized Users.

(b) **Customer Data.** As between Customer and Provider, all rights, including all Proprietary Rights, in and to Customer Data will remain at all times the exclusive property of Customer. These Terms of Service do not grant Provider any rights, title or interest, whether express or implied, in and to any data, content or intellectual property

of Customer or any Customer Data, except for the limited right to transmit and process Customer Data, and then only as expressly stated in these Terms of Service and/or solely to the extent necessary for Provider to fulfill its obligations under these Terms of Service. In no event will Provider gain any rights, title or interest, whether express or implied, in and to any Customer Data as the result of any transmitting and/or processing of such Customer Data.

(c) **Network Flow Data.** As between Customer and Provider, all rights, including all Proprietary Rights, in and to Network Flow Data will remain at all times the exclusive property of Customer. These Terms of Service do not grant Provider any rights, title or interest, whether express or implied, in and to any Network Flow Data, except as expressly stated in these Terms of Service and/or solely to the extent necessary for Provider to fulfill its obligations under these Terms of Service.

(d) **Services Ownership.** Notwithstanding anything to the contrary, as between Customer and Provider, all Proprietary Rights in and to the Services themselves shall remain at all times the exclusive property of Provider.

4.2 Data Privacy.

(a) Provider shall ensure that all its personnel who have access to Network Flow Data, Attack Data and Edge Router Sampling Data use reasonable efforts to treat such data as sensitive information.

(b) Provider will use Network Flow Data, Attack Data or Edge Router Sampling Data specific to Customer only for the purpose of fulfilling its duties under these Terms of Service. Provider shall only provide access to, share with, or disclose such data to those employees and Provider Contractor/Agents who need access to the data to fulfill Provider's obligations under these Terms of Service. Provider may not share Network Flow Data, Attack Data or Edge Router Sampling Data specific to Customer with any third party other than a Provider Contractor/Agent.

(c) Provider will only store Network Flow Data, Attack Data or Edge Router Sampling Data for one hundred twenty (120) days, upon which Provider will securely delete all such data that no Person will be able to reasonably locate or extract the data from the Services following such deletion.

4.3 Data Security.

(a) Provider will use commercially reasonable practices, including administrative, physical, and technical safeguards, intended to secure all facilities used to process any data contemplated in these Terms of Service (and such data itself) against unauthorized access, disclosure, alteration, and use. Provider will (i) use commercially reasonable security tools and technologies in connection with the Services and (ii) use commercially reasonable software application protection security technologies in any Provider software.

(b) Whenever there is a Security Incident, Provider will: (i) promptly notify any Customers affected by the Security Incident of the Security Incident within seventy two (72) hours of the occurrence of same; (ii) promptly investigate the Security Incident at Provider's expense; (iii) promptly provide affected Customers with detailed information about the Security Incident uncovered as a result of the investigation or otherwise known to Provider; (iv) promptly provide Provider's remediation plan; (v) promptly take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident; (vi) take appropriate corrective action to prevent the recurrence of a similar Security Incident in the future; and (vii) provide affected Customers with a post Security Incident report.

4.4 Legal Requests.

(a) Upon Provider's receipt of a Legal Request in connection with any Data under these Terms of Service, Provider will, to the extent permitted under applicable law, promptly attempt to redirect the requesting third-party to Customer. If Provider's redirecting efforts are unsuccessful, and, if not prohibited by applicable law from doing so, Provider will, prior to disclosure, provide as much notice of the Legal Request to Customer (which notice will include, if permitted by applicable law, a copy of the Legal Request) as is reasonably practicable to allow Customer to seek a protective order or other legal options.

(b) If Provider receives a legal demand to provide information about Customer under the Communications Assistance for Law Enforcement Act, 18 U.S.C. §2522, Provider will, to the extent permitted under applicable law, promptly notify Customer, and provide Customer all other information reasonably requested in the demand relating thereto, including the point of contact at the Department of Justice in connection with such matter, if applicable.

5 REPRESENTATIONS AND WARRANTIES; DISCLAIMERS

5.1 Warranties.

(a) The Parties represent and warrant to each other that each has, and will maintain, in force insurance intended to protect from the conduct, acts or omissions of its employees, agents and contractors.

(b) Provider represents, warrants and covenants to Customer that: (i) it is an Equal Opportunity Employer; (ii) it has not been barred in any jurisdiction from contracting as a result of a conviction for bid-rigging or bid rotating or as a result of a conviction or admission of bribery or attempted bribery; and (iii) to Provider's knowledge, no officer, director, partner or other managerial agent has been convicted of a felony under the Sarbanes-Oxley Act of 2002 or under any state or federal securities laws within five (5) years from the date hereof.

(c) Notwithstanding anything to the contrary contained in these Terms of Service, Provider further represents, warrants and covenants to Customer that: (i) the Services are conduit services and therefore provides a transmission and processing services solely for the purpose of DDOS attack detection and mitigation for data such as Customer Data, (ii) Provider's processing of any Customer Data over the Services is only transient in nature and only in the form of IP packets, and (iii) any storage of Customer Data would be temporary and only as necessary for the performance of the Services or as required by law.

(d) Without limiting Customer's rights set forth in the next sentence with respect to a breach by Provider of Section 5.1(d), if Provider gains any access to Customer Data in process, other than transient access for the purpose of providing the Services, stores, other than temporarily for purpose of providing the Services, or otherwise takes any action with respect to, Customer Data, that is not related to providing the Services, Provider shall immediately (i) provide written notice of the same to the Customer and (ii) unless otherwise directed by the Customer, delete such Customer Data such that no person shall be able to reasonably locate or extract such Customer Data from the Service after it is deleted. If Provider breaches Section 5.1(d), Customer shall have the right to immediately terminate these Terms of Service and any related Service Order and Service Term.

5.2 Disclaimers.

(a) Provider does not endorse and is not responsible or liable for, the services or features provided by any Customer Applications and/or Third Party Applications that Customer might install or utilize in connection with the Service except to the extent that such Third Party Applications are provided by Provider. Customer acknowledges and agrees that Provider shall not be responsible or liable, directly or indirectly, for any damage or loss caused or alleged to be caused by or in connection with use of or reliance on any Customer Applications and/or Third Party Applications.

(b) If provided, Feedback is provided "AS IS" and Customer does not warrant or otherwise promise that any such Feedback, or the use thereof, will not violate the intellectual property rights of any Person or applicable law.

(c) EXCEPT AS EXPRESSLY SET FORTH IN THESE TERMS OF SERVICE TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE SERVICES ARE PROVIDED "AS IS," AND PROVIDER MAKES NO (AND HEREBY DISCLAIMS ALL) WARRANTIES, REPRESENTATIONS, OR CONDITIONS, WHETHER WRITTEN, ORAL, EXPRESS, IMPLIED OR STATUTORY, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, TITLE, NONINFRINGEMENT, OR FITNESS FOR A PARTICULAR PURPOSE, WITH RESPECT TO THE USE, MISUSE, OR INABILITY TO USE THE SERVICE (IN WHOLE OR IN PART). PROVIDER DOES NOT WARRANT THAT ALL ERRORS CAN BE CORRECTED, OR THAT OPERATION OF THE SERVICE SHALL BE UNINTERRUPTED OR ERROR-FREE.

6 LIMITATION OF LIABILITY

6.1 Types of Damages. TO THE EXTENT LEGALLY PERMITTED UNDER APPLICABLE LAW, NEITHER CUSTOMER NOR PROVIDER NOR ANY OF THEIR RESPECTIVE AFFILIATES, AGENTS, CONTRACTORS OR SUB-CONTRACTORS/PROCESSORS, WILL BE LIABLE FOR ANY SPECIAL, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING IN CONNECTION WITH THESE TERMS OF SERVICE, OR ANY DAMAGES OR COSTS DUE TO LOSS OF PROFITS, DATA, USE OR GOODWILL, PERSONAL OR PROPERTY DAMAGE RESULTING FROM OR IN CONNECTION WITH THESE TERMS OF SERVICE OR THE USE, MISUSE, OR INABILITY TO USE THE SERVICES OR OTHER PRODUCTS HEREUNDER, REGARDLESS OF THE CAUSE OF ACTION OR THE THEORY OF LIABILITY, WHETHER IN TORT, CONTRACT, OR OTHERWISE, EVEN IF ADVISED OF THE LIKELIHOOD OF SUCH DAMAGES OR SUCH POSSIBILITY WAS REASONABLY FORESEABLE. IN NO EVENT SHALL PROVIDER BE LIABLE FOR PROCUREMENT COSTS OF SUBSTITUTE PRODUCTS OR SERVICES OR LOSS OF DATA. THE FOREGOING LIMITATION ON LIABILITY SHALL, HOWEVER, NOT BE APPLICABLE TO (a) A PARTY'S INDEMNITY OBLIGATIONS UNDER THESE TERMS OF SERVICE TO THE EXTENT SUCH DAMAGES ARE AWARDED TO THIRD PARTIES OR (b) ANY VIOLATION BY PROVIDER OF CUSTOMER'S PROPRIETARY RIGHTS (FOR CLARITY, LOSS OF DATA SHALL NOT BE DEEMED A VIOLATION OF CUSTOMER'S PROPRIETARY RIGHTS), OR (c) A PARTY'S WILLFUL MISCONDUCT. FOR CLARITY, A PARTY'S FAILURE TO PERFORM INDEMNITY OBLIGATIONS UNDER THESE TERMS OF SERVICE RESULTS IN DIRECT DAMAGES.

6.2 Amount of Damages. TO THE EXTENT PERMITTED BY APPLICABLE LAW AND EXCEPT AS PROVIDED IN SECTION 6.4, PROVIDER'S AND CUSTOMER'S LIABILITY UNDER THESE TERMS OF SERVICE, IRRESPECTIVE OF THE NUMBER OF CLAIMS UNDER, ARISING OUT OF OR IN ANY WAY CONNECTED TO THESE TERMS OF SERVICE SHALL BE LIMITED TO THE GREATER OF (I) FIVE THOUSAND DOLLARS (\$5,000), OR (II) THE FEES PROVIDER RECEIVED DIRECTLY IN CONNECTION WITH THE PARTICULAR CUSTOMER'S USE OF THE SERVICE DURING THE TWELVE MONTHS IMMEDIATELY PRECEDING THE APPLICABLE CLAIM (AS SUCH AMOUNTS ARE DETERMINED BETWEEN INTERNET2 AND PROVIDER AND REGARDLESS OF WHETHER SUCH AMOUNTS ARE KNOWN TO CUSTOMER).

6.3 TO THE EXTENT PERMITTED BY GOVERNING LAW, NOTWITHSTANDING ANYTHING TO THE CONTRARY CONTAINED IN THESE TERMS OF SERVICE, IN NO EVENT WILL ANY OF THE EMPLOYEES, OFFICERS, TRUSTEES, DIRECTORS, PARTNERS, BENEFICIARIES, JOINT VENTURERS, AUTHORIZED ORGANIZATIONS, STOCKHOLDERS OR OTHER PRINCIPALS OR REPRESENTATIVES OF PROVIDER OR CUSTOMER, DISCLOSED OR UNDISCLOSED, THEREOF, EVER BE PERSONALLY LIABLE TO THE OTHER PERSON (I.E., EITHER CUSTOMER OR PROVIDER, AS APPLICABLE) (INCLUDING FOR DIRECT OR CONSEQUENTIAL DAMAGES), AND THE PARTIES HEREBY WAIVE THE RIGHT TO RECOVER DAMAGES FROM ANY SUCH PERSONS. THE FOREGOING SENTENCE DOES NOT APPLY TO AN INDIVIDUAL PERSON IN THE EVENT OF WILLFUL MISCONDUCT OR FRAUD BY SUCH INDIVIDUAL, OR TO AN EMPLOYEE WHEN SUCH EMPLOYEE IS ACTING OUTSIDE THE SCOPE OF HIS OR HER EMPLOYMENT.

6.4 The limitations on liability contained in Section 6 shall apply regardless of whether the liability is based on breach of contract, tort (including negligence), strict liability, breach of warranties, or any other legal theory, and regardless of whether a Claim is made during or after the Term. Notwithstanding the foregoing, the monetary limitations on liability in Section 6.2 shall not apply as to Provider: (i) with respect to the indemnification obligations of Provider under these Terms of Service; or (ii) to violation by Provider of Customer's Proprietary Rights (for clarity, loss of Data shall not be deemed a violation of Customer's Proprietary Rights). In addition, the monetary limitations on liability in Section 6.2 shall not apply as to Customer: (i) with respect to the indemnification obligations of Customer under these Terms of Service; (ii) with respect to any breach of Sections 2.1 and/or 2.2; (iii) for claims of fraudulent misrepresentation by Customer; or (iv) to violation by Customer of Provider's Proprietary Rights.

7 INDEMNIFICATION

7.1 By Provider.

(a) Provider shall defend Customer Indemnitees from and against all third-party Claims (i) alleging that the Services infringe upon, misappropriate, or violate the Proprietary Rights of such third party; and (ii) for unauthorized access of Data stored by Provider in the Service Portal and resulting from Provider's gross negligence. For clarity, Section 7.1(a)(ii) applies only to unauthorized access of Data where the applicable security incident occurs within Provider's systems; Section 7.1(a)(ii) does not apply (and nothing requires Provider to defend,

indemnify or otherwise be liable in any way) from any failure of the Services to prevent a security incident with respect to Data that is not stored by Provider in the Service Portal.

(b) Provider shall indemnify and hold harmless Customer Indemnitees (i) from and against all Damages finally awarded by a court, arbitrator or tribunal of proper jurisdiction to a third-party claimant and incurred by Customer Indemnitees in connection with any third-party Claims expressly specified in Section 7.1(a), and (ii) for any settlement of third-party Claims expressly specified in Section 7.1(a), where the settlement is agreed to by Provider and Customer each in its sole discretion. Notwithstanding the foregoing, Provider shall not be required to provide such indemnification where the infringement, misappropriation, or violation of the Proprietary Rights of a third party to the extent arising from (1) the Customer Data, (2) Customer's or Customer's Authorized Users' use of the Service in a manner in contravention of the Documentation, or (3) products or services not supplied by Provider.

(c) PROVIDER'S INDEMNIFICATION PURSUANT TO THIS SECTION 7.1 WILL BE PROVIDER'S SOLE AND EXCLUSIVE LIABILITY AND CUSTOMER INDEMNITEES' SOLE AND EXCLUSIVE REMEDY FOR ANY THIRD-PARTY CLAIMS INDEMNIFIABLE BY PROVIDER UNDER THIS SECTION 7.1.

7.2 By Customer.

(a) If Customer is a Subscriber, Customer shall defend Provider from and against all third-party Claims under, arising out of, or related to Customer's breach of Section 2.2 of these Terms of Service to the extent allowable by Virginia law. Nothing herein shall be construed as an express or implied waiver of Customer's sovereign immunity.

(b) If Customer is a Subscriber, to the extent allowable by Virginia law, Customer shall indemnify and hold harmless Provider from and against all Damages finally awarded by a court, arbitrator or tribunal of proper jurisdiction to a third-party claimant and incurred by Provider in connection with (i) any third-party Claims expressly specified in Section 7.2(a), and (ii) for any settlement of third-party Claims expressly specified in Section 7.2(a) where the settlement is agreed to by Customer and Provider each in its sole discretion. Nothing herein shall be construed as an express or implied waiver of Customer's sovereign immunity.

(c) CUSTOMER'S INDEMNIFICATION PURSUANT TO THIS SECTION 7.2 WILL BE CUSTOMER'S SOLE AND EXCLUSIVE LIABILITY AND PROVIDER'S SOLE AND EXCLUSIVE REMEDY FOR ANY THIRD-PARTY CLAIMS INDEMNIFIABLE BY CUSTOMER UNDER THIS SECTION 7.2.

7.3 As a condition to the indemnifying Party's obligations under this Section 7, the indemnified Party will give prompt notice to the indemnifying Party of any Claim, provided that failure to do so will not be deemed a breach of these Terms of Service, but such failure will not relieve the indemnifying Party of its indemnity obligation if such delay does not prejudice the defense thereof. As a condition to its obligations under this Section 7, the indemnifying Party shall have full and complete control over the defense and settlement of any Claim, provided that it will not, without the indemnified Party's prior written approval (which shall not be unreasonably withheld, delayed or qualified), enter into any settlement agreement that admits fault on the part of indemnified Party or its indemnitees or requires the indemnified Party or its indemnitees to make any payment.

7.4 If the indemnifying Party so requests and as a condition to its obligations under this Section 7, at the indemnifying Party's cost and expense, the indemnified Party will provide the indemnifying Party with reasonable assistance with the defense of any Claim. In addition, at the indemnified Party's option, cost, and expense, the indemnified Party shall have the right to participate in the defense of any Claim with counsel selected by the indemnified Party.

8 SERVICE TERM; SUSPENSION AND TERMINATION

8.1 Provider will provide the Services to Customer during the Service Term.

8.2 Provider will have the right to suspend or terminate a Customer's access to the Services (i) if such Customer's or such Customer's Authorized User's use of the Services is an Abuse or otherwise represents a threat to Provider's network; (ii) to the extent necessary to comply with Applicable Law; (iii) if a breach of the Terms of Service has taken or is taking place as determined by Provider; or (iv) Internet2 is in breach or default of its applicable payment and/or other material obligations under the Facilitation Agreement. To the extent possible, Provider will provide Internet2, who will in turn notify Customer, with reasonable advance notice of any suspension

or termination of a Customer's access to the Services and the reason for such suspension or termination, and an opportunity to discuss the matter with Provider and remedy the event giving rise to suspension before such suspension occurs, unless such delay will materially harm Provider's network, or enable unauthorized access to Customer Data (in which cases Provider will notify Internet2, who will in turn notify Customer of such suspension once it has occurred via e-mail).). In the event the suspension is caused by Internet2's breach or default pursuant to Section 8.2(iv), then subject to Provider having the relevant Customer's contact details, Provider will notify Customer directly to enable Customer an opportunity to discuss the matter with Provider. If a Service is suspended, Provider will extend the Service by the length of the suspension period at the end of the Service Term for no extra charge. For the avoidance of doubt, while a Service is suspended, the Customer will not be protected by the Service.

8.3 Provider may also suspend the Service if Provider has a good faith belief that such a course of action is reasonably necessary to mitigate a material damage or liability that may result from Authorized User's or Customer's continued use of the Service. Following a suspension under this 8.3, Provider shall restore the Service as quickly as reasonably possible and extend the Service by the length of the suspension period at the end of the Service Term for no extra charge. For the avoidance of doubt, while a Service is suspended, the Customer will not be protected by the Service.

8.4 As to any suspension permitted in Section 8.2 and 8.3, Provider will (i) use reasonable efforts to suspend only the minimum portion of the Services necessary to address the issues giving rise to the suspension; and (ii) suspend the provision of the Services to only the Authorized User(s) or Customer(s) whose actions necessitated the suspension, if at all practicable.

8.5 In the event of (a) a termination of the FA, or (b) any other agreement that, directly or indirectly, authorized the sale of Services to Customer (e.g., the applicable Tenant Customer Agreement or Internet2 Subscriber Agreement) Customer may continue to receive Services from Provider under these Terms of Service if (1) within ten (10) days prior to the termination or expiration of (a) or (b), as applicable, Customer notifies Provider that it wishes to continue receiving Services under these Terms of Service, and (2) Customer and Provider are able to reach mutually agreeable terms (including pricing) for the continuation of the Services. If Customer continues to receive Services in accordance with the foregoing sentence, Internet2 shall have no responsibilities or obligations under these Terms of Service.

8.6 Either Party may terminate these Terms of Service and any related Service Order or Service Term upon notice to the other Party if the other Party breaches a material term of these Terms of Service and such breach remains uncured within thirty (30) days after receipt of notice of the breach by the non-breaching Party.

9 MISCELLANEOUS

9.1 These Terms of Service and any action related thereto will be governed and interpreted by and under the laws of, and venue will be located in, (i) if Customer is an institution of higher education or an agency of the Commonwealth of Virginia, the state in which Customer's main campus or office is located, or, otherwise (ii) the State of New York, without giving effect to any conflicts of laws principles. The United Nations Convention on Contracts for the International Sale of Goods does not apply to these Terms of Service.

9.2 Reserved.

9.3 If any provision of these Terms of Service is held to be invalid or unenforceable, the other provisions of these Terms of Service will remain enforceable, and the invalid or unenforceable provision will be deemed modified so that it is valid and enforceable to the maximum extent permitted by law.

9.4 Any waiver or failure to enforce any provision of these Terms of Service on one occasion will not be deemed a waiver of any other provision or of such provision on any other occasion.

9.5 Customer shall not assign or otherwise transfer its rights or obligations under these Terms of Service, without obtaining the prior written consent of Provider, and any attempted assignment, subcontract, delegation, or transfer in violation of the foregoing will be null and void. Provider may assign or transfer its rights and obligations

under these Terms of Service, without Customer's consent, in connection with the sale of all, or substantially all, of its stock, business or assets to which the Services relate, and will provide notice to Customer of such assignment or transfer. These Terms of Service shall be binding upon Provider and Customer and their respective successors and permitted assigns.

9.6 Provider will at all times comply with the SLA and shall be fully responsible for providing all support services related to the Services to Customers to the extent expressly set forth in the SLA. For purposes of Customer claims for service credit under the SLA, Provider shall be responsible for (i) validating any Customer claims and (ii) performing the service credit calculation. Provider shall provide to Internet2 the service credit calculation for Customer and credit to Internet2 the corresponding amount in the form of additional Service days at the end of the Service Term. Internet2 shall be responsible for communicating any service credit days to the Customer.

9.7 Notwithstanding anything to the contrary, neither Provider nor Customer will not be deemed in breach of these Terms of Service or otherwise liable or responsible for any event or circumstances beyond its reasonable control (including, without limitation, Internet outages or labor disputes).

9.8 Notwithstanding anything to the contrary in any agreement, except as set forth in Section 9.6 and 9.12 and except for Internet2's notification obligations in Sections 8.2 and 3.3, these Terms of Service will not be deemed to create any obligations, rights, or liabilities for Internet2.

9.9 Provider may issue public statements and press releases regarding, or otherwise publicly discussing, these Terms of Service and/or the relationship between Customer and Provider, subject to Customer's prior written approval, which shall not be unreasonably withheld or delayed.

9.10 The provisions of these Terms of Service, which by their nature are continuing, shall continue in full force and effect and shall bind the Parties beyond any termination of these Terms of Service, including the following: Sections 1.1, 2.1, 4, 5.1(c), 5.1(d), 5.2, 6, 7, 8, 9 (other than Section 9.5 and 9.9), and 10.

9.11 Provider shall have the right to use Contractor/Agents to perform any of its obligations or to act on behalf of such Person. All actions of Provider's or Customer's Contractors/Agents in connection with these Terms of Service are attributable to such Person for all purposes under these Terms of Service.

9.12 Upon termination of these Terms of Service, any liabilities accrued before the effective date of the termination will survive. For clarity purposes, if such termination is a result of a breach by Provider to Sections 3.3, 5.1(d) or 8.6 of these Terms of Service, Customer shall have the right to terminate its Service Order and Service Term without any further requirement to pay for the remaining unused Service Term and Provider shall refund to Internet2 the pro rata portion of any pre-paid fees that Internet2 paid for Customer's use of the Service. Internet2 shall be responsible for providing any resulting refund to Customer.

9.13 These Terms of Service will not be construed to create an association, joint venture or partnership between Customer and Provider or to impose any partnership liability upon Customer or Provider.

9.14 Notwithstanding anything to the contrary, notices to be provided pursuant to Sections 3.3, 4.4, 5.1(d), 7.3, 8.6, and 9.5 of these Terms of Service, (a) by Provider shall, without limitation, be deemed to have provided such notice or information by emailing the email address that Customer specifically designates in writing to Provider as its recipient for information or notice pursuant to these Terms of Service. Provider shall have no obligations to provide any notice under these Terms of Service if Customer does not designate such an email address and, in such case, notice to Customer shall not be deemed a condition precedent to any right of Provider under these Terms of Service and (b) by Customer shall, without limitation, be deemed to have provided such notice or information by emailing Provider at HannahM@Radware.com or GilG@Radware.com.

9.15 These Terms of Service, including all Attachments, constitutes the entire agreement and understanding between the Parties with regard to the Services and supersedes any and all prior agreements, communications, or discussions, oral or written, between the Parties relating to the Services. These Terms of Service may not be amended, modified, or changed, except by a writing signed by both Parties.

9.16 In the event of any inconsistency between the terms and conditions of these Terms of Service and the terms and conditions of the Subscriber Agreement between Internet2 and Customer, or a Tenant Customer Agreement between a Subscriber and a Tenant, the terms and conditions of these Terms of Service will govern and prevail over the terms and conditions of the Subscriber Agreement or Tenant Agreement. In the event of any inconsistency between the terms and conditions of these Terms of Service and the terms and conditions of the SLA, the terms and conditions of the SLA will govern and prevail over the terms and conditions of these Terms of Service.

10 DEFINITIONS

Capitalized terms shall have the meanings set forth in this Section 10 or in the Section where they are first used.

10.1 **"Abuse"** means any of the following impermissible uses of the Service: (a) causing, aiding, encouraging, or facilitating a domain or URL hosted by Provider for Customer (or any Customer end user) to point to or otherwise direct traffic or any material in violation of any applicable law or regulation; (b) using or encouraging, aiding or facilitating the use of the Service (including by pointing to web sites or locations) to (i) create, transmit, distribute or store material that: violates trademark, patent, copyright, trade secret or other intellectual property laws; violates the privacy, publicity or other personal rights of others; (ii) include tools designed for compromising security (including but not limited to password guessing programs, cracking tools or network probing tools); (iii) violate export control, data protection or anti-terrorism laws; impair the privacy of communications; or that is obscene, pornographic, harassing, threatening, abusive or discriminatory or which encourage hatred against an identifiable group; or are defamatory or knowingly contain viruses; or constitute a criminal offense or give rise to civil liability; (c) using the Service in such a manner as to directly or indirectly negatively affect Provider or Provider's network (including, without limitation, overloading servers on the Provider network or causing portions of the Provider network to be blocked); (d) attempting to penetrate or manipulate, or encourage, aid or facilitate the penetration or manipulation of, the security features of the Provider network or any other system (including but not limited to unauthorized access to or use of data, systems or networks; probing, scanning or testing the vulnerability of a system or network; breaching security authentication measures; unauthorized monitoring of data or traffic; interference with the service of any user, host or network by any means; forging any TCP/IP packet header or any part of a message header); (e) posting article(s) or substantively similar articles(s) to an excessive number of newsgroups using a Provider hosted domain or posting such messages through a Service; (f) sending unsolicited and/or mass e-mailings, whether or not such activities provoke complaints from the recipients (Provider has a zero tolerance policy on the sending of SPAM, junk e-mail or unsolicited commercial email and email may not contain forged headers or fake contact information); or (g) utilizing or causing the utilization of an excessive amount of Provider network resources with excessiveness being determined by Provider in Provider's sole discretion.

10.2 **"Attack Data"** means metadata collected during or derived from an attack on Customer's traffic that Customer has routed through the Service and the related log created by the Service and stored via the Service Portal for access by Customer.

10.3 **"API" or "Application Programming Interface"** means the interfaces and protocols that are provided by Provider to Customers for the purpose of Customers' development of solutions and applications that can operate with the Services on an automated or scripted basis.

10.4 **"Authorized Users"** means, with respect to a Subscriber, such Subscriber's employees and Contractor/Agents or Tenants who are authorized by Subscriber to access the Services and with respect to a Tenant, such Tenant's employees and Contractor/Agents.

10.5 **"Claim(s)"** means, individually and collectively, claims, actions, demands, suits, or proceedings.

10.6 **"Contractor/Agents"** means, with respect to Customer or Provider, such Person's independent contractors, subcontractors, sub-processors, or other non-employees that perform any of such Person's obligations hereunder or act on behalf of such Person in connection with these Terms of Service.

10.7 **"Customer"** means the Subscriber or Tenant accessing the Service.

- 10.8 “Customer Applications”** means, as to any Customer, applications developed by that Customer that connect to the Provider Service via the API.
- 10.9 “Customer Data”** means all data, inclusive of metadata but exclusive of Network Flow Data, including Personal Data and all binary text, sound, image, video or other files, including applications, that are uploaded to, transmitted by, accessed by or processed by the Service by, or on behalf of, Customer through Customer’s use of the Services.
- 10.10 “Customer Indemnitees”** means, collectively, Customer who is a Subscriber, its successors, assigns, affiliates and subsidiaries and each of their respective members, managers, directors, officers, shareholders, agents, employees and representatives.
- 10.11 “Damages”** means, individually and collectively, damages, costs, liabilities, and losses and expenses, including reasonable attorneys’ fees.
- 10.12 “Data”** means, collectively, Attack Data, Edge Router Sampling Data, Event Data, Customer Data, Network Flow Data, Network Service Data, and Personal Data.
- 10.13 “Data Controller”** means as such term or like terms is defined in the Privacy & Data Security Laws.
- 10.14 “Data Processor”** means as such term or like terms is defined in the Privacy & Data Security Laws.
- 10.15 “Data Protection Code of Conduct”** means Provider’s Data Protection Code of Conduct attached hereto as Attachment 3.
- 10.16 “Documentation”** means Provider’s published specifications, user manuals, other technical materials relating to the Service, and use guidelines or other restrictions adopted by Provider and made available to Customer from time to time.
- 10.17 “Edge Router Sampling”** means the random packet sampling and inspection of Customer traffic performed by the Service for Customers using edge router monitoring.
- 10.18 “Edge Router Sampling Data”** means any metadata associated with Customer’s traffic based on the Edge Router Sampling and the related log created and stored via the Service Portal for access by Customer.
- 10.19 “Event Data”** means all information relating to the type, nature, identity, signature, source, frequency, reputation and other characteristics of traffic and activity derived or compiled from Attack Data and Edge Router Sampling Data, if applicable, by Provider in the course of performing the Service.
- 10.20 “Facilitation Agreement”** means the Master Service Agreement for DDoS Services entered into between Provider and Internet2.
- 10.21 “Feedback”** means any suggestions, enhancement requests, feedback, or recommendations provided by Customer to Provider to improve the Services.
- 10.22 “FERPA”** means the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g, and its implementing regulations.
- 10.23 “Internet2 Subscriber Agreement”** means the agreement with respect to the Services between a Subscriber and Internet2.
- 10.24 “Legal Request”** means a request pursuant to applicable law (including any public records law or regulation) purporting to require disclosure of any data implicated under these Terms of Service.

10.25 “Network Flow Data” means digital records that describe and characterize connections made over a network or are otherwise contained in an IP packet, including data elements such as IP addresses and port numbers for source and destination endpoints, protocols, traffic volume, timestamps, and network interfaces utilized, but excluding the content of communications between endpoints.

10.26 “Network Service Data” means all analytical products, including models, reports, and analyses, created or derived by Provider in connection with the delivery of the Services. Network Service Data may be compiled, analyzed or otherwise derived from Network Flow Data, aggregated network traffic utilization and performance data, and/or other server activity data collected by Provider in the course of performing the Service. Network Service Data does not include any Customer Data or Personal Data.

10.27 “Party” means Provider and Customer individually. Collectively, they are “Parties”.

10.28 “Person” means an individual, partnership, corporation, limited liability company, university, trust, decedent’s estate, joint venture, joint stock company, association, unincorporated organization, governmental body or agency, or other entity.

10.29 “Personal Data” includes personal identifiers such as name, address, phone number, date of birth, Social Security Number, and student or personnel identification number; personally identifiable information contained in student education records as that term is defined under FERPA; driver’s license number; other state or federal identification numbers such as passport, visa or state identity card numbers; account number or credit or debit card number, or an account number or credit card number in combination with any required security code, access code or password that would permit access to an individual’s financial account; and such other data and information as may be specified by applicable law as “personal data” or the equivalent thereof.

10.30 “Personal Information” means as such term or like terms is defined in the Privacy & Data Security Laws.

10.31 “Privacy & Data Security Laws” means all applicable privacy and data protection laws, rules, regulations, best practices and regulatory guidance relating to privacy, data security, cybersecurity and Personal Information.

10.32 “Proprietary Rights” means any patent, copyright, trademark, trade secret or other intellectual property right.

10.33 “Protected Assets” means the set of Customer’s protected objects, network segments and servers including but not limited to domain names, individual IP addresses and IP networks, which are protected by the Service.

10.34 “Provider” means Radware, Inc., with a place of business located at 575 Corporate Drive Mahwah, New Jersey.

10.35 “Qualified Person(s)” means (a) a higher education member of Internet2, (b) an Internet2 Research and Education Network Member, (c) a K-12 educational institution, higher education institution, library, museum, or other not-for-profit organization that in Internet2’s reasonable judgment has or facilitates a research or educational mission, or (d) other institutions as agreed to in a signed writing by Internet2 and Provider.

10.36 “Scrubbing Center” means the cloud-based data center facilities operated by or on behalf of Provider in order to deliver the Service.

10.37 “Section 2.2(b) of the FA” means Section 2.2(b) of the Facilitation Agreement.

10.38 “Security Incident” means: (a) any unlawful or unauthorized access to any Network Flow Data, Attack Data and/or Edge Router Sampling Data stored on equipment used by or on behalf of Provider or in facilities used by or on behalf of Provider; or (b) any unlawful or unauthorized access to any equipment used by or on behalf of Provider or in facilities used by or on behalf of Provider that has resulted in, or Provider reasonably expects may result in,

loss, disclosure or alteration of any Network Flow Data, Attack Data and/or Edge Router Sampling Data or any such equipment or facilities.

10.39 "Service" means the services provided by Provider under these Terms of Service as set forth in Attachment 1.

10.40 "Service Data" means (a) Network Service Data, (b) Event Data, and (c) Feedback collected by Provider in the course of performing the Service. Service Data will not include any Customer Data or Personal Data.

10.41 "Service Level" means each of the performance criteria set out in the SLA with regard to the Service.

10.42 "Service Order" means the document or order form used between Customer and Internet2 to order the Services.

10.43 "Service Portal" means a Customer facing web-based application which displays Service data relevant to the Customer and allows Customer to perform various Service configurations and utilize various functions.

10.44 "Service Start Date" means, for each Service, the date of the onboarding of a Subscriber or a Tenant, as evidenced from a successful diversion test or within thirty (30) days of the anticipated Service Start Date provided by Provider after reviewing the requested Service Start Date in the Service Order, whichever is earlier, unless such delay beyond the thirty (30) days is caused by the Provider.

10.45 "Service Term" means the fixed term designated in a Service Order, for a specific Customer which may be terminated solely in accordance with these Terms of Service. The Service Term will commence on the Service Start Date.

10.46 "SLA" means the Provider Service Level Agreement attached as Attachment 2.

10.47 "Subscriber" means any Qualified Person that enters into an Internet2 Subscriber Agreement with Internet2 as contemplated in, and consistent with, the terms of the Facilitation Agreement.

10.48 "Tenant" means a Qualified Person to whom Subscriber resells the Services, as contemplated in, and consistent with, the terms of the Internet2 Subscriber Agreement between Internet2 and Subscriber. With respect to each Subscriber, Tenant does not include other networks that are deemed a Protected Asset who do not purchase Services from Subscriber.

10.49 "Tenant Customer Agreement" means the agreement with respect to the Services between a Subscriber and Tenant.

10.50 "Third Party Applications" means any Third Party software or application.

10.51 "Traffic Redirection Command Policy" means as such term is defined in the SLA.

Acknowledgment

Patricia K. Branscome _____ hereby acknowledges receipt of these Radware Terms of Service and agrees to be bound by the terms thereof.

Patricia K. Branscome
49FF589E7C9243B...
[Signature]

3/9/2020

[Date]

Patricia K. Branscome

[Name Printed]

Attachment 1

Description of Services

On-Demand Cloud DDoS Protection Service that protects against Volumetric DDoS Attacks only and is activated manually on-demand when the attack threatens to saturate the Customer's Internet pipe and provided by Provider pursuant to these Terms of Service including the terms of the Service Level Agreement.

Attachment 2

RADWARE SERVICE LEVEL AGREEMENT (SLA)

1. **Service Levels.** Provider will provide the Service pursuant to the Service Levels described in this Section 1.
 - 1.1. **Service Uptime Service Level.**
 - 1.1.1. The Service will be available on a 99.999% annual basis.
 - 1.2. **Time-To-Diversion-Initiation Service Level.**
 - 1.2.1. Provider will initiate a diversion of the Customer's traffic from the Protected Assets that are under a DDoS Attack to the Provider's Scrubbing Center(s), within the timeframe set forth in Section 1.2.3 below.
 - 1.2.2. The Time-To-Diversion-Initiation is dependent on the diversion method utilized. Provider and Customer expect utilizing on Manual Diversion, for which the following will apply.
 - 1.2.2.1. **Manual Diversion.** Manual Diversion of the Customer's traffic from the Protected Assets that are under a DDoS Attack to the Provider's Scrubbing Center(s), will be triggered when the Customer provides Provider with a Volumetric DDoS Attack notification via the Service Portal or support hotline. The Time-To-Diversion-Initiation for a Manual Diversion will commence once Provider is notified by the Customer about a Volumetric DDoS Attack and requests the diversion. In order to request a Manual Diversion, the Customer must provide Provider both the Customer contact and the Protected Assets that the Customer request to divert manually.
 - 1.2.3. Time-To-Diversion-Initiation will be 15 minutes.
 - 1.2.4. Notwithstanding the Service Level in Section 1.2.3 above, the Time-To-Diversion-Initiation may vary and is dependent on Internet conditions, Customer's and Internet2's systems that may block or delay account, network and configuration changes, and other conditions over which Provider has no control. Additionally, in some cases, the Customer and/or Internet2 may be required to first take certain actions in order to enable the diversion. Customer acknowledges and agrees that Provider shall not be deemed to have failed the Time-To-Diversion-Initiation Service Level in the event the failure is resulting from any of these varying conditions and/or from (i) Customer's failure to notify Provider pursuant to Section 1.2.2.1 or, (ii) in a BGP diversion method advertisement/route withdrawal during an attack mitigation, a Customer's or the Customer's ISP's failure to withdraw BGP advertisement of the protected network in order to allow the BGP redirection.
 - 1.3. **Time-To-Mitigation Service Level.**
 - 1.3.1. Provider will mitigate attacks within the timeframes defined in Section 1.3.2 below. The Time-To-Mitigation period will commence once 75% or more of the Customer's traffic from the Protected Assets that are under a DDoS Attack has been successfully diverted to the Provider's Scrubbing Centers and will end upon reaching Consistency-Of-Mitigation. Notwithstanding the foregoing, Time-To-Mitigate will re-commence when the DDoS Attack is morphed and/or when the Attack Vectors change and end when the Consistency-Of-Mitigation is reached.
 - 1.3.2. Time-To-Mitigation will vary depending on the DDoS Attack type, as follows:

	Time-To-Mitigation					
	UDP / ICMP Floods	SYN Floods	TCP Flag Abuses	GET / POST Floods	DNS Reflection	DNS Flood Attack
On-Demand	5 min	5 min	5 min	15 min	10 min	10 min

1.3.3. Following the End of Attack, traffic will remain diverted for an additional Cooling Period of up to 4 hours, after which the diversion will be deactivated if no additional attacks have been detected. In some cases, the Customer and/or Internet2 may be required to take action in order to deactivate the diversion.

1.4. Consistency-Of-Mitigation Service Level.

1.4.1. Provider will provide a Consistency-Of-Mitigation level of no less than 95%. Consistency-Of-Mitigation is defined as being the proportion of the traffic that is forwarded to Customer's Protected Assets via the Service that is clean.

1.4.2. The Consistency-Of-Mitigation measurement window is defined as being the period following the Time-To-Mitigation and the End of Attack.

1.4.3. If Customer believes Provider is in breach of Consistency-Of-Mitigation Service Level, Customer should provide to Provider a packet capture of at least one hour in duration that identifies total attack traffic volumes as a proportion of the total traffic volume received from the Service for the period identified as failing to meet defined Service levels.

2. Provider Obligations.

2.1. Provider warrants that it shall endeavor to maintain the availability of Customer inbound Internet connectivity via the Service on a best effort basis.

2.2. Provider shall maintain a team of networking professionals, information security specialists and DDoS Attack experts to support the Service on 24/7/365 basis.

2.3. Provider shall cease traffic diversion within a 4-hour period (at Provider's sole discretion) following the End of Attack upon which ingress traffic will revert to being routed directly to Customer.

2.4. Regular maintenance work performed on the Provider systems that support the Service and/or the Scrubbing Centers, shall only be performed during specific periods. These regular "Maintenance Windows" are scheduled on the 1st day of each calendar month and run between 00:00 and 06:00 hours in the time zone in which a specific Scrubbing Center is located. During these regular "Maintenance Windows" Provider will make available an alternate Scrubbing Center to deliver the Service. If Provider needs to conduct non-Emergency Maintenance work outside of a scheduled regular Maintenance Window, it will do so after having provided Customer with seven (7) days written notice about the work and the potential for interruption to the Service. Provider shall not be obligated to inform Customer in advance of Emergency Maintenance work.

3. Remedies.

3.1. **Service Outage.** Customer will be eligible for remedies if Provider fails to meet any of its Service Levels as defined in Section 1 of this SLA; provided, such failure directly results in a Service Outage, and the Customer reports the Service Outage to Provider and Internet2 within five (5) calendar days of the commencement of the Service Outage event via email to Internet2 and Provider. Provider shall determine in its sole discretion exercising good faith whether Provider’s failure to meet its Service Level caused a Service Outage using its records, data and other evidence. Remedies for valid Service Outage claims will be in the form of additional Service days, to be provided at the end of the Service Term, as follows:

Service Outage Occurrence	Time elapsed since a Service interruption resulting from failure to meet the Service Levels became a Service Outage	Remedy
Single event within a calendar month	Less than 3 hours	1 day credit of monthly Service per Service Outage
Single event within a calendar month	More than 3 hours but less than 72 hours	3 days credit of monthly Service per Service Outage
Multiple events within 3 calendar months	Events greater than 45 minutes (at least one event in any 10 days)	Material Breach – Customer can terminate Service

3.2. **General Remedy Terms.**

3.2.1. The foregoing Service credits shall not be applicable during the first 21 days of operation following the initiation of the Service.

3.2.2. In order to qualify for any remedies, the Customer (through Internet2) must be in good financial standing with Provider with all accounts current.

3.2.3. The sum of credits for multiple events shall not exceed 25% of the monthly Service days for any single calendar month.

3.2.4. Customer shall be entitled to only a single credit should any one incident result in a failure of more than one of the Service Levels.

3.2.5. In the event that a Service Outage occurs as a result of a Special Unavailability event, the occurrence shall not qualify for remedial credits.

3.2.6. ANY CREDITS AWARDED BY PROVIDER HEREUNDER SHALL BE CUSTOMER’S SOLE AND EXCLUSIVE REMEDY FOR ANY FAILURE BY PROVIDER TO MEET ANY SERVICE LEVEL.

4. **Cloud ERT Service.** Provider will provide Customer its Cloud Emergency Response Team (ERT) Standard Service.

5. **Definitions.**

5.1. “Agreement” means the Master Service Agreement for DDoS Services entered into between Provider and Internet2.

- 5.2. "Attack Duration" is the duration of a DDoS Attack on the Customer's Protected Assets, commencing from the attack Detection to the end of the Cooling Period following the End of Attack. "Attack Vector" means the type of a DDoS Attack which includes but is not limited to the attack method, attack tools, network level (3,4,7) of the attack, source IP address(es), destination(s) (Protected Asset(s) and/or port(s)), packets per second rate, and bits per second rate.
- 5.3. "Certainty Support Guide" means the Certainty Support Guide as published by Provider from time to time at: <https://www.radware.com/support/certainty-support-program/>.
- 5.4. "Cloud ERT Standard Service" means as defined and described in Section 4 above and in Provider's Certainty Support Guide.
- 5.5. "Cooling Period" means a period of time during which Provider announces End of Attack and normal Peace Time traffic routing patterns are resumed. The Cooling Period duration is limited to 4 hours or up to the moment that the Customer's Link Utilization drops below 65% of the Customer's internet capacity bandwidth.
- 5.6. "Customer" means a Qualified Person that enters into an Internet2 Subscriber Agreement or a Tenant Customer Agreement (which agreement includes the Radware Terms of Service) contemplated in, and consistent with the terms of the Agreement.
- 5.7. "DDoS Attack" means a Distributed Denial of Service attack that targets the Customer's Protected Assets.
- 5.8. "Degraded Availability of Protected Assets" refers to a period of more than 60 continuous minutes during which, as a result of an attack, the Service fails to perform as designed and Customer IT assets - including but not limited to Internet connectivity, website(s), servers, and applications - exhibit degraded performance. The determination of whether or not there exists or existed a Degraded Availability of Protected Assets shall be made by Provider in its sole and absolute discretion.
- 5.9. "Detection" means identification of one of the following events as a result of a DDoS Attack: (i) Internet Link Utilization >90% for a Utilization Measurement Period of 5 minutes; (ii) Internet Link Utilization >75% for a Utilization Measurement Period of 10 minutes; or (iii) the Customer's Link Utilization Threshold is reached or exceeded.
- 5.10. "Emergency Maintenance" means any activity that Provider, at its sole discretion, deems necessary to avert a situation that poses an immediate risk to the continued operation of the Service. The Provider shall not be obligated to inform the Customer in advance of Emergency Maintenance work.
- 5.11. "End of Attack" means the time at which an attack is judged to have been aborted. The precise time is deemed to be when inbound Internet Link Utilization levels drop to 65% or below and/or when they drop to a level below Customer's typical inbound Internet Link Utilization levels for the time of day and day of week, whichever Link Utilization level is higher.
- 5.12. "Force Majeure" means acts or events beyond either party's reasonable control. Force Majeure may include, by way of example but not limitation, those circumstances beyond the control of the affected such as acts of God, the public enemy, acts of government, or any governmental department or agency thereof, as well as fire, flood, earthquakes, epidemics, quarantines, riots, wars, civil insurrections, freight embargoes.
- 5.13. "Internet2 Subscriber Agreement" means an agreement entered into between a Customer that is a Subscriber and Internet2.

- 5.14. "Link Utilization" means the amount of traffic traversing the Customer's internet link leading to the Customer's Protected Asset(s) divided by the total capacity of such internet link, measured over a certain period of time and expressed in percentage.
- 5.15. "Link Utilization Threshold" means a value, expressed in percentage that represents the upper bound of the Customer's Link Utilization, which the Customer and Provider predefine during the on-boarding.
- 5.16. "Non-Volumetric DDoS Attack" means a DDoS Attack when the Link Utilization Threshold is not reached over the length of the Utilization Measurement Period.
- 5.17. "Peace Time" means any time that is not Attack Duration and or Cooling Period.
- 5.18. "Protected Assets" means the set of Customer's protected objects, network segments and servers including but not limited to domain names, individual IP addresses and IP networks, which are protected by the Service.
- 5.19. "Qualified Person(s)" means (a) a higher education member of Internet2, (b) an Internet2 Research and Education Network Member, (c) a K-12 educational institution, higher education institution, library, museum, or other not-for-profit organization that in Internet2's reasonable judgment has or facilitates a research or educational mission, or (d) other institutions as agreed to in a signed writing by Internet2 and Provider.
- 5.20. "Scrubbing Center" refers to cloud-based data center facilities operated by or on behalf of Provider in order to deliver the Service.
- 5.21. "Service" means the following: (i) Provider's On-Demand DDoS mitigation service that protects against Volumetric DDoS Attacks only and is activated on-demand when the attack threatens to saturate the Customer's Internet pipe and provided by Provider pursuant to the terms of this SLA; and (ii) the Cloud ERT Standard Service described in Section 4 above and as further defined in the Glossary.
- 5.22. "Service Level" means each of the performance criteria set out in Section 1 of this SLA with regard to the Service.
- 5.23. "SLA" means this Service Level Agreement.
- 5.24. "Service Outage" means an interruption of the Service as a result of Provider's failure to meet any of the Service SLA's that results in: (i) the total lack of availability of Protected Assets for a period of at least 30 minutes; or (ii) Degraded Availability of Protected Assets for a period in excess of 1 hour.
- 5.25. "Special Unavailability" refers to an outage event of the Service due to: (i) network unavailability, including telecommunications failures that are used to connect Provider Scrubbing Centers to Customer Protected Assets; (ii) problems with Customer's domain name registrar; (iii) problems with Protected Assets; (iv) Customer misuse; (v) other negligent or unlawful acts by Customer or its agents or its Providers; (vi) any other action or inaction by a third party; or (vii) Force Majeure. The cause of such an outage event shall be determined in good faith by Provider.
- 5.26. "Subscriber" means any Qualified Person that enters into an Internet2 Subscriber Agreement with Internet2 as contemplated in, and consistent with, the terms of the Agreement.
- 5.27. "Tenant" means a Qualified Person to whom Subscriber resells the Services, as contemplated in, and consistent with, the terms of the Internet2 Subscriber Agreement between Internet2 and Subscriber. With respect to each Subscriber, Tenant does not include other downstream customers who do not purchase Services from Subscriber.

- 5.28. "Tenant Customer Agreement" means the agreement with respect to the Services between a Subscriber and Tenant.
- 5.29. "Terms of Service" means the Radware Terms of Service that are attached as an exhibit to the Agreement, an Internet2 Subscriber Agreement or a Tenant Customer Agreement.
- 5.30. "Traffic Redirection Command Policy" means the method by which traffic is redirected from Customer's Protected Assets to Provider's Scrubbing Center facilities in the event of a DDOS Attack. One option exists, BGP Model. Upon DDOS Attack, Provider and/or Customer shall initiate the process to redirect inbound Internet traffic to Provider's Scrubbing Center facilities.
- 5.31. "Utilization Measurement Period" means a period of time, measured in consecutive minutes, that the Customer and Provider predefine during the on-boarding and over which the Customer's average Link Utilization Threshold will be measured and calculated.
- 5.32. "Volumetric DDoS Attack" means a DDoS Attack when the Link Utilization Threshold is reached or exceeded over the length of the Utilization Measurement Period.

Attachment 3
Provider's Data Protection Code of Conduct



Data Protection Code of Conduct

May 2018



Radware Data Protection Code of Conduct

Version 1.0

Version Control

Version	Date	Developed by	Change	Approved by
1	10/5/2018	Gadi Meroz, Vice President & General Counsel Signature: _____	Initial version	Roy Zisapel, Chief Executive Officer and President Signature: _____



Radware Data Protection Code of Conduct

Version 1.0

Table of Contents

Overview	4
1.1. Definitions	4
1.2. Purpose	4
1.3. Scope	4
1.4. Radware Contact Details	5
Ways in which Data will be Processed	6
1.5. Data Processing Contract	6
1.6. Collection of Personal Data	6
Record Keeping	6
Data Protection Requirements	7
1.8. Lawful, Fair and Transparent Processing	7
1.9. Data Security Measures	8
1.10. Personal Data Breach	9
1.11. Data Privacy by Design and by Default	9
1.12. Transfer of Personal Data to Third Countries	10
1.13. Sub-Processing	11
1.14. Law Enforcement/Governmental requests	11



Radware Data Protection Code of Conduct

Version 1.0

1. Overview

1.1. Definitions

Capitalized terms shall have their meanings in the Regulation (EU) 2016/679 (General Data Protection Regulation).

- 1.1.1. **Personal Data** means any information relating to an identified or identifiable natural person ('data subject'); 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;
- 1.1.2. **Processing** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- 1.1.3. **Controller** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
- 1.1.4. **Processor** means a natural or legal person, public authority, agency or other body, which processes personal data on behalf of the controller.

1.2. Purpose

- 1.2.1. This Code of Conduct (or "Code"), as defined in GDPR Article 40, documents Radware's commitment to information privacy and personal data protection practices.
- 1.2.2. This Code of Conduct describes the level of privacy protection that Radware will provide to its cloud customers.
- 1.2.3. The purpose of the Code is to ensure our customers that the services that they wish to use are suitable for the data processing activities that they wish to perform.
- 1.2.4. This Code does not replace a contract between Radware and its customer.

1.3. Scope

- 1.3.1. The Code deals with Radware's Cloud Services.
- 1.3.2. Radware's Cloud Services provide a range of fully managed, enterprise-grade services

Confidential Property of Radware



Radware Data Protection Code of Conduct

Version 1.0

including:

- 1.3.2.1. **Cloud WAF Service** provides continuously adaptive web security protection. Radware's ICSA Labs certified, web application firewall, provides wide coverage of the OWASP Top-10 threats and automatically adapts a customer's protection to evolving threats and the protected assets
 - 1.3.2.2. **Cloud Malware Protection** defends organizations against zero-day malware by analyzing data collected from a global community of two million users using patented machine learning algorithms to detect previously unknown malware based on their unique behavior patterns.
 - 1.3.2.3. **Cloud DDoS Protection Services** provides enterprise-grade DDoS protection in the cloud and delivers wide security coverage with accurate detection and short time to protection from today's most dynamic and constantly evolving DDoS threats.
 - 1.3.2.4. **Cloud Web Acceleration Service** delivers accelerated web application response time and enables the application service to provide proactive, automated protection from advanced threats.
- 1.3.3. Radware serves as the Processor for the above mentioned services.

1.4. Radware Contact Details

1.4.1. Corporate information:

- 1.4.1.1. Address: 22 Raoul Wallenberg Street, Tel-Aviv, 6971917, Israel
 - 1.4.1.2. Phone: 972-3-766-8666
 - 1.4.1.3. Fax: 972-3-766-8982
 - 1.4.1.4. URL: www.radware.com
- 1.4.2. For any question or complaint concerning data privacy, please contact Gadi Meroz, VP & General Counsel, DPO@radware.com.



Radware Data Protection Code of Conduct

Version 1.0

2. Ways in which Data will be Processed

2.1. Data Processing Contract

- 2.1.1. Radware shares with its cloud customers the Cloud Services Agreement or other binding legal act, which govern the processing carried out on behalf of our customers and set out the subject matter and duration of the processing, the type of personal data and categories of data subjects and the obligations and rights of the cloud customer.

2.2. Collection of Personal Data

- 2.2.1. Radware is agnostic to the actual personal information captured by its cloud services and does not process the personal data included in the cloud services as such. The nature of personal data collected in accordance with the above-mentioned services may vary depending on the activity and may include.

- 2.2.1.1. Customer's web stream may include personal data
- 2.2.1.2. Samples of network traffic may include personal data
- 2.2.1.3. Captures of session traffic may include personal data
- 2.2.1.4. IP Addresses
- 2.2.1.5. Userids

3. Record Keeping

Radware maintains a record of processing activities.

3.1. That record contains all of the following information:

- 3.1.1. the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
- 3.1.2. the purposes of the processing;
- 3.1.3. a description of the categories of data subjects and of the categories of personal data;
- 3.1.4. the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organizations;
- 3.1.5. where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
- 3.1.6. where possible, the envisaged time limits for erasure of the different categories of data;
- 3.1.7. The Record is drawn up in cooperation with all relevant operational departments and the

Confidential Property of Radware



Radware Data Protection Code of Conduct

Version 1.0

Data Protection Officer (or "DPO").

- 3.1.8. The record is kept in writing, including in electronic form.
- 3.1.9. Radware will re-assess the accuracy of the Records on a regular basis in view of updating these where appropriate.

4. Data Protection Requirements

The purpose of this section is to clarify Radware's role as a processor under EU General Data Protection Regulation (GDPR) in the context of its cloud based services.

4.1. Lawful, Fair and Transparent Processing

- 4.1.1. Protecting the rights of data subjects for private data sent to Radware's cloud services is the sole responsibility of the customers.
- 4.1.2. Radware will process personal data in accordance with the customer's instructions.
- 4.1.3. The Service Level Agreement and use by the customer of the features and functionalities made available by Radware as part of the service are the customer's complete and final instructions to Radware in relation to processing of personal data.
- 4.1.4. For processes under its control (when it serves as a controller) Radware only processes private data if:
 - 4.1.4.1. The data subject has given consent to the processing of his or her personal data for one or more specific purposes;
 - 4.1.4.2. Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
 - 4.1.4.3. Processing is necessary for compliance with a legal obligation to which the controller is subject;
 - 4.1.4.4. Processing is necessary in order to protect the vital interests of the data subject or of another natural person;
 - 4.1.4.5. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
 - 4.1.4.6. Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, which require protection of person, al data, in particular where the data subject is a child.
- 4.1.5. For private data residing in processes under its control, Radware is responsible for making privacy notices understandable and accessible. This information is communicated to the data subjects in an intelligible form using clear and plain language. The specific

Confidential Property of Radware



Radware Data Protection Code of Conduct

Version 1.0

information that is provided to the data subject include:

- 4.1.5.1. the identity and the contact details of the controller and, if any, of the controller's representative;
- 4.1.5.2. the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- 4.1.5.3. the period for which the personal data will be stored;
- 4.1.5.4. the existence of the rights to request access, rectification, erasure or to object to the processing, and the conditions (or lack of conditions) relating to exercising these rights, such as whether the lawfulness of previous processing will be affected;
- 4.1.5.5. the categories of personal data concerned;
- 4.1.5.6. the recipients or categories of recipients of the personal data, where applicable;
- 4.1.5.7. Where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data.

4.2. Data Security Measures

4.2.1. **IS Program** - Radware maintains an information security program with the aim to

4.2.1.1. Identify reasonably foreseeable and internal risks to the security of Radware Network, and

4.2.1.2. Minimize security risks, including through risk assessments and regular testing.

4.2.2. **CISO** - Radware has designated a Chief Information Security Officer (CISO) to coordinate and be accountable for the information security management system.

4.2.3. **Security Reviews** - Radware conducts periodic reviews of the security of its infrastructure and the adequacy of its information security program.

4.2.4. **Baseline for the management system** - Radware follows best practices for its security Information Security Management system (ISMS) and is certified for ISO 27001, ISO 27017, ISO 27018 and ISO 27032. Radware is also certified for ISO 28000 Supply Chain Security and ISO 9001 Quality Management. PCI Service Provider and HIPAA compliance is confirmed by an annual self-assessment.

4.2.5. **Human Resources** - Radware ensures that employees, contractors, partners and vendors understand their data protection and security responsibilities. All employees of the organization and where relevant, contractors receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.

4.2.6. Access Control

4.2.6.1. Radware ensures that only authorized users will have access to its information assets and to private data. Users are only be provided with access to assets that

Confidential Property of Radware



Radware Data Protection Code of Conduct

Version 1.0

they have been specifically authorized to use.

- 4.2.6.2. Radware provides the customers with an access control management system for the relevant cloud management portals as part of the service.
- 4.2.7. **Encryption** - Radware ensures proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information, Radware will ensure that confidential data will be encrypted whenever extracted from their primary repository.
- 4.2.8. **Physical and Environmental Security** - Radware will use physical and environmental measures to prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.
- 4.2.9. **Operational & Communication Security** - Radware will maintain appropriate controls related to management of IT production including change management, capacity management, malware, backup, logging, monitoring and vulnerabilities management.
- 4.2.10. **System acquisition, development and maintenance** - Radware maintains security throughout the lifecycle of the information systems.
- 4.2.11. **Supplier Relationship** - Radware ensures that its partners, suppliers and contractors are maintaining adequate security measurements to secure Radware and its customers' information, through contracts and periodic audits as necessary.

4.3. Personal Data Breach

- 4.3.1. Radware detects security incidents through automated detection capabilities such as network-based and host-based IDPSs, antivirus software, and log analyzers, and through manual means, such as problems reported by users.
- 4.3.2. Any individual who suspects that a theft, breach or exposure of personal data, customer's data or Radware's confidential data has occurred must immediately report the incident and provide a description of what occurred in a <TICKETING-SYSTEM> ticket. The report should include full and accurate details of the incident.
- 4.3.3. If the incident is related to personal information breach, it is reported to the DPO.
- 4.3.4. In the event that the breach of personal information is confirmed, the DPO must report the breach to the supervisory authorities within 72 hours.
- 4.3.5. In the case of a personal data breach, the DPO, without undue delay and no later than 72 hours after confirming the breach of personal data, will notify the breach to the supervisory authority.
- 4.3.6. In addition, Radware will notify the relevant controllers without undue delay after becoming aware of a personal data breach.
- 4.3.7. If the breach could result in a high risk to the rights and freedoms of the affected users, the users must also be notified. Consider the dangers of 'over-notifying'.

4.4. Data Privacy by Design and by Default

Confidential Property of Radware



Radware Data Protection Code of Conduct

Version 1.0

- 4.4.1. Radware considers security and privacy during system or software analysis and design and implements appropriate measures, designed to implement data-protection principles, such as data minimization, in an effective manner and it integrates the necessary safeguards into the processing in order to protect the rights of data subjects.

4.5. Transfer of Personal Data to Third Countries

- 4.5.1. Radware provides European customers with the ability to choose to use the service to store and process its data entirely within the EEA.
- 4.5.2. Radware will provide to the customer information about the region and country where its data is stored and processed by or on behalf of Radware, including if its sub-contracts part of the processing to third parties.
- 4.5.3. Radware will provide to the customer information about the region and country where its data is stored and processed by or on behalf of Radware, including if Radware subcontracts part of the processing to third parties.
 - 4.5.3.1. For security reasons, only a general location (such as a city or city region area) will be provided. This general description shall, at least, allow the customer to identify which EU Member State has jurisdiction over the customer for processing performed by the customer using the service.
 - 4.5.3.2. For services which can be run indifferently within several different locations in Radware's Network, Radware makes the information easily accessible to the customer and enable customers to select the location(s) within Radware's Network where their data will be processed.
- 4.5.4. Radware may transfer personal data outside the EEA without applying the previously mentioned restrictions when:
 - 4.5.4.1. the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards (i.e. it is insufficient to just mention that data will be transferred to a third country);
 - 4.5.4.2. the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
 - 4.5.4.3. the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party;
 - 4.5.4.4. the transfer is necessary for the establishment, exercise or defense of legal claims;
 - 4.5.4.5. the transfer is necessary to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;

Confidential Property of Radware



Radware Data Protection Code of Conduct

Version 1.0

4.6. Sub-Processing

- 4.6.1. Radware maintains an up-to-date list of sub-processors authorized to access customer data.
- 4.6.2. Subject to applicable law, Radware will obtain the customer's consent before authorizing a third party sub-processor to access and process customer data.
- 4.6.3. If the customer objects to a sub-processor, the customer may immediately terminate the Service Agreement for convenience or, if agreed by the customer and Radware, immediately terminate the service or that part of the service, which is provided by Radware using the relevant sub-processor.
- 4.6.4. Radware imposes on other processors the same data protection obligations stipulated between Radware and the cloud customer, by way of a contract (or other binding legal act), in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of EU applicable law;

4.7. Law Enforcement/Governmental requests

- 4.7.1. Radware will not disclose customer data to a third country law enforcement agency unless it is necessary to comply with a valid and legally binding court judgment or governmental or court order or request.
- 4.7.2. Radware will not disclose more customer data than is necessary to comply with the relevant court judgment, or governmental or court order or request.
- 4.7.3. If Radware receives a valid and legally binding court judgment, order, or request from any law enforcement or governmental authority to disclose customer data, then, unless prohibited by law, Radware will inform the customer before disclosure to provide the customer with the opportunity to seek protection from disclosure.