**F5 END USER SERVICES AGREEMENT**

**SERVICE-SPECIFIC TERMS**

**Last Updated: August 5th, 2024**

The Service-Specific Terms below supplement and are incorporated in and form a part of your agreement with us governing your use of the SaaS Offerings (the "Agreement"). Capitalized terms used in these Service-Specific Terms but not defined below are defined in the End User Services Agreement located at https://www.f5.com/pdf/customer-support/eusa.pdf or if applicable, entered into between us and you. In the event of a conflict between a provision of these Service-Specific Terms and a provision of the Agreement, these Service-Specific Terms will control with respect to its terms. Your use of any SaaS Offerings to which you have access via a Customer Dashboard shall be subject to the terms of the Agreement, including the applicable Service-Specific Terms herein, regardless of whether you have placed an Order for such SaaS Offerings.

**1. Silverline SaaS Offerings**

**Silverline Operational Terms.**

1.1.1. **Additional Definitions.** Unless otherwise defined in these Service-Specific Terms, the following definitions apply:

"**95th Percentile Calculated Bandwidth**" means your bandwidth calculated as: collecting 5-minute samples over a calendar month based on traffic that is transmitted or received between the F5 Silverline Network and your network, sorting the samples from largest to smallest, discarding the top (highest) 5 percent of samples, and selecting the remaining highest single sample. The selected sample determines the bandwidth at the 95th percentile value.

**"DDoS"** means distributed denial of service.

**"Excessive Use"** of a Silverline SaaS Offering shall have the meaning set forth in the applicable Service-Specific Term.

**"F5 Silverline Network"** means the IP network owned or operated by us related to the Silverline SaaS Offerings and the system(s) (servers, and associated software) deployed by us for the delivery of the Silverline SaaS Offerings. The F5 Silverline Network does not include customer-side web-based user interfaces, zone/data transfer mechanisms, customer-side web servers, application programming interfaces, or other customer accessible data manipulation software, Internet connectivity provided by third parties, the telecommunications means between the servers, nor the Internet routes between servers.

**"Silverline SaaS Offerings"** means the Silverline DDoS Protection Service; the Silverline Shape Defense Service; the Silverline Web Application Firewall Service; and/or any other services made available as Silverline SaaS Offerings from us from time to time, as applicable. If you order Silverline SaaS Offerings under the Agreement, all references to "SaaS Offerings" therein shall be deemed include the Silverline SaaS Offerings.

**"Silverline DDoS Protection Service"** means the distributed denial of service protection service delivered through the F5 Silverline cloud-based platform. The Silverline DDoS Protection Service is also governed by the Silverline DDoS Protection Service-Specific Terms.

**"Silverline Shape Defense Service"** means the automated threat protection service delivered through the F5 Silverline cloud-based platform. The Silverline Shape Defense Service is also governed by the Silverline Shape Defense Terms.

**"Silverline Web Application Firewall Service"** means the web application firewall service delivered through the F5 Silverline cloud-based platform. The Silverline Web Application Firewall Service is also governed by the Web Application Firewall Service-Specific Terms.

**"SOC"** means the F5 Silverline security operations center.

1.1.2. **Ordering Silverline SaaS Offerings Through Distribution.** Unless otherwise agreed to in writing by us, you will procure Silverline SaaS Offerings from an Authorized Distribution Partner in accordance with the Agreement and the terms between you and such Authorized Distribution Partner. You and F5 shall enter into an Order describing the Silverline SaaS Offerings to be purchased by you from the Authorized Distribution Partner, and You will submit purchase orders to an Authorized Distribution Partner (a list of which is available from us upon request). All terms relating to Silverline SaaS Offerings ordering, payment, taxes and fees will be as set forth in your agreement with such Authorized Distribution Partner.

1.1.2.1. **Excessive Use.** We may monitor your use of the Silverline SaaS Offerings for Excessive Use. If your usage of the Silverline SaaS Offerings is deemed Excessive Use, as measured by us, you will (i) negotiate in good faith with us to increase the capacity of such Silverline SaaS Offerings to cover such Excessive Use, and (ii) place additional orders for the applicable Silverline SaaS Offering to remedy the Excessive Use.

1.1.2.2. **Service Term – Subscription Start Date.** The Service Term for the Silverline SaaS Offerings shall start on the Subscription Start Date. "Subscription Start Date" shall mean (a) with respect to an initial Order of any Silverline SaaS Offering, the date that we have approved the purchase order for such Silverline SaaS Offerings, which date shall be no later than fifteen (15) business days following the date that (i) you have

signed or accepted the Agreement, and (ii) we have received the applicable Order; provided, however, that you may request a Subscription Start Date that is later than the date provided in this Section 1.4 if such later Subscription Start Date, clearly labeled as such, is set forth in the applicable Order; and (b) with respect to the renewal of any Silverline SaaS Offerings, the day immediately following the last day of the prior Service Term.

1.1.2.3. **Service Term – Under Attack.** Notwithstanding Section 1.4 of this Service-Specific Term, if you order Silverline SaaS Offerings while under a DDoS attack, the Subscription Start Date shall start on the date that you have accepted this Agreement, including all applicable Orders, for the applicable Silverline SaaS Offering. You hereby acknowledge and agree that you are obligated to promptly place an order for such Silverline SaaS Offering with us or an Authorized Distribution Partner, as applicable, and pay applicable fees for such Silverline SaaS Offering.

1.1.2.4. **Security.** During any Service Term, we shall implement a security program for the applicable Silverline SaaS Offering that is designed to comply with the Payment Card Industry Data Security Standard (PCI-DSS) or any similar industry security standard. Upon your written request, which shall not be made more than once in any twelve (12) month period, we shall provide you a PCI-DSS, or other similar security standard, attestation of compliance, or similar certification of compliance, applicable to the Silverline SaaS Offerings provided hereunder.

1.1.2.5. **New Data.** Certain Silverline SaaS Offerings allow you to receive data from us that we own or license from a third party, or that we create through proprietary analysis and modeling of Customer Data alone or in combination with other data, such as risk score, intelligence about a threat from some source other than Customer Data, or substantiation of either of the foregoing (collectively, "New Data"). New Data does not include Customer Data. As between you and us, we own and retain all rights, title and interest in and to the New Data, and you may use New Data only for your lawful, internal cybersecurity analysis/auditing purposes in accordance with this Agreement. You are responsible for proper security of any New Data you receive. Unless prohibited by law, you will promptly inform us of any request from a third party to exercise any purported rights with respect to the New Data.

1.1.2.6. **Service Level Agreement.** During the Service Term and provided that you are compliant with the Agreement and any Service-Specific Terms, we will use commercially reasonable efforts to provide the applicable Silverline SaaS Offerings in accordance with the Service Level Agreement.

**2. Silverline DDoS Protection Service**

**Silverline DDoS Protection Service Operational Terms.**

2.1.1. **Additional Definitions.** Unless otherwise defined in these Service-Specific Terms, the following definitions apply:

"**Always Available**" means a Silverline DDoS Protection Service where all prerequisite configuration elements are established and you determine when to, and take action to, divert your traffic to the F5 Silverline Network for DDoS mitigation.

"**Always On**" means a Silverline DDoS Protection Service where your applicable traffic protected from attack is continuously directed to the F5 Silverline Network for DDoS monitoring and mitigation.

"**Clean Bandwidth**" means the 95$^{th}$ Percentile Calculated Bandwidth of traffic returned to, or received from, your premises after the Silverline DDoS Protection Service mitigation methods are applied.

"**Data Center**" means a single physical location or a virtual construct that is used to centralize computing resources. A data center may support multiple applications, or IP Subnets. For the Silverline DDoS Protection Service, 4 (four) clean traffic return paths will be configured for each Customer Data Center (e.g., GRE tunnels).

"**Router Monitoring**" means that we will monitor for Layer 3-4 DDoS events while your traffic is not running through the F5 Silverline Network. Router Monitoring requires you to appropriately configure identified routers to send flow data to us for the purpose of monitoring traffic for DDoS events. The number of your routers configured to transmit flow data to us will determine quantity of Router Monitoring objects.

"**VIP**" means an IP address configuration provided to you by us which includes an IP address allocated by us to process and transmit traffic to defined origin(s) within your Data Center. The VIPs are used in a proxy deployment to enable communication from the Internet to us and then to your application within your Data Center.

2.1.2. **Excessive Use.** For the purpose of this Service-Specific Term, "**Excessive Use**" means your usage of the Silverline DDoS Protection Service in (a) excess of the Clean Bandwidth as measured by 95th Percentile Calculated Bandwidth; or (b) your configuration of Router Monitoring or Data Centers (e.g., GRE Tunnels) exceeds the quantities defined in the applicable Order.

2.1.3. **Additional Disclaimers and Limitations.** SILVERLINE DDOS PROTECTION SERVICES PROVIDE PROTECTION ONLY IN ACCORDANCE WITH THE SPECIFICATIONS ASSOCIATED WITH THE APPLICABLE SILVERLINE DDOS PROTECTION SERVICE, SUBJECT TO YOUR ORDERING AND PAYING APPLICABLE FEES FOR SUCH SAAS OFFERINGS IN ACCORDANCE WITH THE APPLICABLE PAYMENT TERMS, INCLUDING SPECIFICATIONS ON CLEAN BANDWIDTH, NUMBER OF DATA CENTERS, NUMBER OF VIPS, ROUTER MONITORING QUANTITY AND WHETHER SUCH SERVICES ARE ALWAYS ON OR ALWAYS AVAILABLE.

**3. Silverline Shape Defense Service**

**Silverline Shape Defense Operational Terms.**

3.1.1. **Additional Definitions.** Unless otherwise defined in these Service-Specific Terms, the following definitions apply:

**"Authorized Website(s)**" means the Customer's website(s) hosted on the FQDN being monitored by the SaaS Offerings.

"**Authorized Mobile Application(s)**" means the Customer's mobile application(s) hosted on or communicating with the FQDN being monitored by the SaaS Offerings.

"**Client-Side Code**" means any code, program or other software provided by F5 to Customer, such as Java Script software and SDKs, that Customer may deploy on Authorized Websites or Authorized Mobile Application(s) to collect or generate Threat Data.

**"FQDN"** means a fully-qualified domain name which, by means of a domain name system (DNS), points to a single canonical name (CNAME), a single IP address, or a single pool of distributed IP addresses.

"**Threat Data**" means, individually and collectively, indications of compromise, telemetry, behavioral information, device information, network information, data relating to attacks and attack tools, attack credentials and other information relating to the provision, use and performance of various aspects of the Silverline Shape Defense Service and any related services, systems and technologies, including any numeric or logical values generated by the Silverline Shape Defense Service and any contextual information associated with any such values (e.g., any description or the meaning of any such values). Threat Data does not include information that identifies a natural person.

3.1.2. **Excessive Use.** For purposes of this Service-Specific Term, "**Excessive Use**" means your usage of the Silverline Shape Defense Service (a) in excess of the bandwidth provided for in the applicable Order, as measured by us where use shall be excessive if either (i) the 95th Percentile Calculated Bandwidth exceeds the applicable tier defined in the Order; or (ii) you are targeted by a sustained DDoS attack whereby your application consumes more than one DDoS attack that exceeds a peak of 1.5 Gbps of attack traffic during any twelve (12) month period, unless you have an effective subscription to Silverline DDoS Protection SaaS Offerings covering such attack or (b) where you have provisioned a quantity of FQDNs for protection via the Silverline Shape Defense Service greater than the defined amount of FQDNs in the Order. You acknowledge and agree that our obligations are limited to providing the Silverline Shape Defense SaaS Offerings in the quantiles identified in the Order(s) for the active Service Term(s).

3.1.3. **Grant of Right**. Subject to the terms and conditions of the Agreement, any applicable Orders, and the Service Policies, we grant you a limited, non-exclusive, non-transferable, non-sublicensable license during the Service Term to:

3.1.3.1. install and execute the Client-Side Code solely on the Authorized Website(s) and Authorized Mobile Application(s), for the sole purpose of collecting and generating Threat Data and transmitting the Threat Data to the Silverline Shape Defense Service; and

3.1.3.2. if an Order grants you the current right to access and use the Silverline Shape Defense Service: (a) obtain the New Data (defined below) from the Silverline Shape Defense Service; (b) internally use the New Data solely to determine whether fraudulent activities are occurring on the Authorized Website(s) or Authorized Mobile Application(s); and (c) have only those employees of Customer who are principally responsible for fraud detection access any such New Data solely for the purposes of exercising the rights granted in Section 3.1.3.2(b) of these Service-Specific Terms; and, in each case solely for Customers' internal business purposes.

3.1.4. Additional Terms Applicable to Data.

3.1.4.1. **Threat Data**. Notwithstanding anything to the contrary set forth in the Agreement, we will have the right to collect, generate and analyze Threat Data, and we own and retain all right, title and interest worldwide in and to the Threat Data, and all intellectual property rights therein or related thereto. Threat Data does not include Customer Data.

3.1.4.2. **New Data.** Certain of the SaaS Offerings allow you to receive data from us that we own or license from a third party, or that we create through proprietary analysis and modeling of Threat Data and/or Customer Data alone or in combination with other data, such a risk score, intelligence about a threat from some source other than Customer Data, or substantiation of any of the foregoing (the "**New Data**"). New Data does not include Customer Data.

3.1.4.3. **Ownership of and Restrictions on use of Data.** As between you and us, we own and retain all rights, title and interest in and to the New Data, and Threat Data, and you hereby assign to us any right, title and interest you may have or acquire in any New Data and Threat Data. New Data, and Threat Data are F5's Confidential Information. You will use New Data only for your lawful, internal cybersecurity analysis/auditing purposes in accordance with this Agreement. You are responsible for proper security of any New Data you receive or possess. Unless prohibited by law, you will promptly inform us of any request from a third party to exercise any purported rights with respect to the New Data.

3.1.4.4. **Obligations on Termination**. Upon expiration of the Service Term, you will immediately: (i) discontinue use of the New Data; (ii) return to F5, or at F5's written request destroy, all tangible materials containing, reflecting, or incorporating the New Data or any Documentation pertaining thereto; (iii) permanently erase all electronic versions of the foregoing materials from all systems you directly or indirectly control; and (iv) execute and deliver to F5, upon request, written certification of your compliance with the foregoing.

3.1.5. **Restrictions**. Customer will not (and will not authorize or permit any third party to): (a) attempt to reverse engineer the New Data or Threat Data or any portion thereof, or otherwise attempt to derive any processes, techniques, methods, specifications, protocols, algorithms, interfaces, data structures, or other information used to collect or generate any New Data or Threat Data; (b) rent, lease, lend, sell, sublicense, assign, distribute, publish, transfer or otherwise make available any New Data, Threat Data, or Documentation pertaining thereto, or any portion thereof, to any third party, including on or in connection with the Internet or any time-sharing, service bureau, software as a service, cloud or other technology or service or otherwise use any New Data other than as expressly allowed under these Service-Specific Terms; (c) use the New Data or the Documentation pertaining thereto (or any information obtained or derived from the New Data or such Documentation) for the development, provision or use of a competing service or product; (d) externally disclose benchmarking or competitive analysis of any of the New Data or Documentation pertaining thereto; (e) use the New Data in violation of any applicable law or regulation; or (f) allow any person (other than its employees who are principally responsible for fraud detection for the Authorized Website(s) or Authorized Mobile Application(s)) to access or use the New Data or any Documentation pertaining thereto, or any information obtained or derived therefrom.

3.1.6. Service Tier Descriptions.

3.1.6.1. **Silverline Shape Defense SaaS Offerings**. Silverline Shape Defense SaaS Offerings include:

(a) SOC support by phone, chat and email to maintain security policies in support of your covered FQDN(s), including onboarding and configuration of the Silverline Shape Defense Service.

(b) Periodic review of automated threats reported by the Silverline Shape Defense Service against your covered FQDN(s).

(c) Upon yours request, the SOC may also engage with you for Silverline Shape Defense false positive reviews.

3.1.7. **Additional Disclaimers and Limitations.** SILVERLINE SHAPE DEFENSE SERVICES PROVIDE PROTECTION FOR ONLY FQDN(S) ASSOCIATED WITH THE APPLICABLE SERVICES CONTRACTUALLY ASSOCIATED WITH THE SILVERLINE SHAPE DEFENSE SERVICES ON THE APPLICABLE ORDER(S).

3.1.8. Notwithstanding anything to the contrary in the Agreement, liabilities and damages arising out of the following will not be subject to any limitations on liability in the Agreement: Customer's unauthorized use of the Silverline Shape Defense Service, Threat Data, or New Data (including without limitation the exercise of rights in excess of the license grants in Section 3.1.3 of these Service-Specific Terms), or Customer's breach of any of its obligations in Sections 3.1.4.4, or 3.1.5 of these Service-Specific Terms.

**4. Silverline Web Application Firewall Service**

**Silverline Web Application Firewall Operational Terms.**

4.1.1. **Additional Definitions.** Unless otherwise defined in these Service-Specific Terms, the following definitions apply: **"FQDN"** means a fully-qualified domain name which, by means of a domain name system (DNS), points to a single canonical name (CNAME), a single IP address, or a single pool of distributed IP addresses.

4.1.2. **Excessive Use.** For purposes of this Service-Specific Term, "**Excessive Use**" means your usage of the Silverline Web Application Firewall Service (a) in excess of the bandwidth provided for in the applicable Order, as measured by us where use shall be excessive if either (i) the 95th Percentile Calculated Bandwidth exceeds the applicable tier defined in the Order; or (ii) you are targeted by a sustained DDoS attack whereby your application consumes more than one DDoS attack that exceeds a peak of 1.5 Gbps of attack traffic during any twelve (12) month period, unless you have an effective subscription to Silverline DDoS Protection SaaS Offerings covering such attack or (b) where you have provisioned a quantity of FQDNs for protection via the Silverline Web Application Firewall Service greater than the defined amount of FQDNs in the Order. You acknowledge and agree that our obligations are limited to providing the Silverline Web Application Firewall SaaS Offerings in the quantiles identified in the Order(s) for the active Service Term(s).

4.1.3. **Silverline Managed Services.** Only the following section applies only to Silverline's Managed Services offering:

4.1.3.1. **Silverline Managed Web Application Firewall SaaS Offerings**. Silverline Managed Web Application Firewall SaaS Offerings include:

(d) SOC support by phone, chat and email to maintain security policies in support of your covered FQDN(s), including periodic tuning of security policies in accordance with the results of vulnerability assessments as performed against your covered FQDN(s).

(e) Detailed analysis of your web application firewall violation logs for the purpose of tuning the security policies.

(f) Vulnerability assessment data imported from a third party or sources provided by you.

(g) Reporting on web application firewall violation data.

(h) Upon yours request, the SOC may also engage with you for web application firewall violation false positive reviews.

4.1.4. **Additional Disclaimers and Limitations.** SILVERLINE WEB APPLICATION FIREWALL SERVICES PROVIDE PROTECTION FOR ONLY FQDN(S) ASSOCIATED WITH THE APPLICABLE SERVICES CONTRACTUALLY ASSOCIATED WITH THE SILVERLINE WEB APPLICATION FIREWALL SERVICE ON THE APPLICABLE ORDER(S). IN THE EVENT THAT YOU QUALIFY FOR, PURSUANT TO OUR ELIGIBILITY CRITERIA AS MAY BE CHANGED FROM TIME TO TIME IN OUR SOLE DISCRETION, AND ELECT TO EXPORT YOUR WEB APPLICATION FIREWALL POLICIES ("**WAF POLICIES**") FROM

THE SILVERLINE WEB APPLICATION FIREWALL SERVICES FOR USE IN CONNECTION WITH YOUR SEPARATELY LICENSED F5 APPLICATION SECURITY MANAGER SOFTWARE ("**WAF POLICY EXPORT**"), YOU ACKNOWLEDGE AND AGREE THAT SUCH EXPORT AND USE OF THE WAF POLICIES ARE AT YOUR SOLE RISK. WE HEREBY DISCLAIM ALL LIABILITY, EXPRESS OR IMPLIED, IN CONNECTION WITH YOUR WAF POLICY EXPORT, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTIES AGAINST INFRINGEMENT OF THIRD-PARTY RIGHTS, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE (INCLUDING, WITHOUT LIMITATION, DETECTION OF DISTRIBUTED DENIAL OF SERVICE ATTACKS). YOU ACKNOWLEDGE AND AGREE THAT WE HAVE NO OBLIGATION TO PROVIDE SUPPORT TO YOU IN CONNECTION WITH SUCH WAF POLICY EXPORT.

**5. Silverline Data Protection Terms**

**DPA.**

The DPA applies to personal data (as defined under the General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR")) that we process as part of the Silverline SaaS Offerings as detailed below.

**Processing Details and Security.**

For details regarding the processing for the Silverline SaaS Offerings please refer to the DPA and Schedule A below. For a description of the technical and organizational security measures for the Silverline SaaS Offerings, please refer to Schedule B below.

**Schedule A - Silverline SaaS Offerings**

**DETAILS OF THE DATA PROCESSING**

*Details relevant to Annex I(B) of the 2021 Standard Contractual Clauses*

Subject Matter, Nature and Purpose of Processing, and details of processing operations: Provision of the Silverline SaaS Offerings, as described herein.

Term/Duration of Processing: As set forth in the Agreement.

Categories of Data Subjects: Visitors to your Internet-facing websites and mobile applications protected by the Silverline SaaS Offerings

Categories of Data for DDoS, WAF, Shape Defense:

> Internet Protocol (IP) addresses and network traffic data; information from interactions between the user (and their browser or device) and the online property; and other technical data about the browser or device that may be used to screen for malicious activity; Silverline Shape Defense Service identifiers (pseudo-randomly generated values).In addition to IP addresses, Shape Defense also processes pseudo-randomly generated values stored in a first-party cookies.
>
> Special Categories of Data (if any): Not applicable, unless incidentally present in the traffic data that the service analyses for malicious activity. Even if such data were to be present, the SaaS Offering does not use the special aspects of the personal data for any purpose. For example, if the traffic data to be analyzed for malicious activity somehow reflected an identifiable individual's philosophical belief, the SaaS Offering would not track this belief or take it into consideration.

*Additional details relevant to Annex 1(B) of the 2021 Standard Contractual Clauses*

Applied safeguards and restrictions specific to any special categories of data: The same high standard of protection described in these Service-Specific Terms and the DPA applies to this and other categories of personal data.

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

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: Logs of exceptions (i.e., blocking or flagging events) are retained for 12 months.

**Schedule B - Silverline SaaS Offerings**

**TECHNICAL AND ORGANISATION SECURITY MEASURES**

*Annex II of the 2021 Standard Contractual Clauses*

F5's Silverline Data Centers – including those at Singapore and Frankfurt, Germany – maintain, and keep current, substantive compliance with the Payment Card Industry Data Security Standard (PCI DSS). The PCI DSS demands the following key controls:

Network configuration security

Elimination of all default system passwords and other security parameters on all systems used to host or process personal data.

Encrypted transmission of all Personal Data in transit

Functional and regularly updated anti-virus controls on all systems used to host or process Personal Data.

Exclusive use of unique, traceable system IDs on all systems used to host or process Personal Data

Controls to restrict physical access controls to all systems used to host or process Personal Data

Logging and monitoring of all access to Personal Data and systems hosting Personal Data

Regular testing of all security controls

Creation and maintenance of an information security policy, and communication of this policy to all personnel who have access to Personal Data at the F5 Data Centre

Additionally, F5 Silverline production systems maintain strict isolation from the remainder of the F5 environment.

**Access control to premises and facilities**

Technical and organizational measures to control access to premises and facilities, particularly to check authorization, for example:

Access control systems: ID reader; magnetic card; chip card

(Issue of) keys

Door locking (electric door openers etc.)

Security staff

Surveillance facilities: Alarm system; CCTV monitor

**Access control to systems**

Technical (ID/password security) and organizational (user master data) measures for user identification and authentication, for example:

Password procedures: special characters; minimum length; change of password

Automatic blocking: password; timeout

Creation of one master record per user

Encryption of media

**Access control to data**

Requirements driven definition of the authorization scheme and access rights and logging and monitoring of access, for example:

Differentiated access rights: profiles; roles; transactions and objectives

Reports

Access logs

Change logs

Deletion logs

**Disclosure control**

Measures to transport, transmit and communicate or store data on media (manual or electronic) and for subsequent checking, for example:

Encryption / Tunneling: VPN

Electronic signature

Logging

Transport security

**Input control**

Measures for subsequent checking whether data have been entered, change or removed and by whom, for example:

Logging and reporting systems

**Job control**

Technical and organizational measures to segregate the responsibilities between the controller and the processor, for example:

Unambiguous contract wording

Formal commissioning of processing

Criteria for selecting the processor

Monitoring of contract performance

**Availability control**

Measures to assure data security (physical/logical), for example:

Backup procedures

High-Availability storage configurations

Mirroring of hard disks (e.g., RAID technology)

Uninterruptable power supply

Remote storage

Anti-virus

Firewall

Disaster recovery plan

**Segregation control**

Measures to provide for separate processing (storage, amendment, deletion, transmission) of data for different purposes, for example:

"Internal client" concept / limitation of use

Segregation of functions (development/testing/production)

We may replace or modify the measures described above so long as the overall security of the F5 Silverline SaaS Offerings is not materially lowered during a subscription term. Subprocessors may maintain commercially reasonable security through measures that may differ from those set forth above.

**6. NGINX One**

**6.1. Operational Terms.**

6.1.1. Through your subscription to the NGINX One SaaS Offering, you will be provided with (a) the ability to configure your NGINX software product(s) ("**NGINX Software**") via the Customer Dashboard, and (b) limited access to certain SaaS Offerings as reflected in your Order. While your use of such SaaS Offerings is governed by the Agreement, your use of the NGINX Software is governed by the End User License Agreement located at https://www.f5.com/pdf/customer-support/end-user-license-agreement.pdf or such other signed agreement containing applicable end user license terms for use of the NGINX Software ("**EULA**").

6.1.2. Service Level Agreement. Neither the NGINX Software nor the functionality of the Customer Dashboard which enables you to configure your NGINX Software is subject to the Service Level Agreement or any other service levels under the Agreement.

6.2. Data Protection Terms

6.2.1. **DPA.** The DPA applies to personal data (as defined under the General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR")) that we process as part of the NGINX One SaaS Offering, as detailed below.

6.2.2. **Processing Details and Security.** For details regarding the processing for NGINX One SaaS Offering, please refer to the DPA and Schedule A below. For a description of the technical and organizational security measures for the NGINX One SaaS Offering, please refer to Schedule B below.

**Schedule A – NGINX One**

**DETAILS OF THE DATA PROCESSING**

*Details relevant to Annex I(B) of the 2021 Standard Contractual Clauses*

Subject Matter, Nature and Purpose of Processing, and details of processing operations: Configuring the NGINX Software, as described herein.

Term/Duration of Processing: As set forth in the EUSA.

Categories of Data Subjects: Those identified by IP address or otherwise if included in configuration files.

Categories of Data: [Internet Protocol (IP) addresses and any other personal information stored in configuration files, if any. Special Categories of Data (if any): Not applicable.

Applied safeguards and restrictions specific to any special categories of data: Not applicable.

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

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: Personal data is retained during the license term. The data will be removed after termination, subject to a reasonable period of retention of copies made for backup and business continuity purposes.

**Schedule B – NGINX One**

**TECHNICAL AND ORGANISATION SECURITY MEASURES**

*Annex II of the 2021 Standard Contractual Clauses*

We will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of your Personal Data, as described in the controls included in the following:

Service Organization Control 2 Report designed to meet the applicable criteria for the security, availability and confidentiality principles set forth in TSP Section 100A, Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy by the American Institute of Certified Public Accountants.

The applicable requirements of the Payment Card Industry – Data Security Standard version 4.0.

We may replace or modify the measures described above so long as the overall security of the NGINX One service is not materially lowered during a subscription term.

Subprocessors will maintain commercially reasonable security through measures that may differ from those set forth above.

**7. Terms Applicable to the following SaaS Offerings (collectively "BRM SaaS Offerings"): Distributed Cloud Authentication Intelligence; Distributed Cloud Aggregator Management; Distributed Cloud Client-Side Defense; Application Traffic Insight; Distributed Cloud Account Protection; Distributed Cloud Bot Defense (Managed Service); and Distributed Cloud Data Intelligence**

**Operational Terms.**

7.1.1. **Additional Definitions**. Unless otherwise defined in these Service-Specific Terms, the following definitions apply:

**"Appliance**" means a hardware device onto which we have pre-installed Software components of the SaaS Offerings to which you subscribe under an Order.

"**Authorized Website(s)**" means the Customer's website(s) being monitored by the SaaS Offerings.

"**Authorized Mobile Application(s)**" means the Customer's mobile application(s) being monitored by the SaaS Offerings.

"**Client-Side Code**" means any code, program or other software provided by F5 to Customer, such as Java Script software and SDKs, that Customer may deploy on Authorized Websites or Authorized Mobile Applications to collect or generate Threat Data.

"**Derived Data**" means any learnings, algorithms, know-how or other data or information derived from or any improvements to the Threat Data and any intellectual property rights therein, in each case, developed or created by or for you.

"**Licensed Threat Data**" means that subset of the Threat Data that Customer is authorized to receive from F5 in connection with Customer's subscription to the Distributed Cloud Data Intelligence SaaS Offerings as permitted by the applicable Order.

"**Threat Data**" means, individually and collectively, indications of compromise, telemetry, behavioral information, device information, network information, data relating to attacks and attack tools, attack credentials and other information relating to the provision, use and performance of various aspects of the SaaS Offerings and any Software and related services, systems and technologies, including any numeric or logical values generated by the SaaS Offerings and any contextual information associated with any such values (e.g., any description or the meaning of any such values). Threat Data does not include information that identifies a natural person.

**"Transaction"** means, as measured by F5's systems: (i) for Distributed Cloud Bot Defense (Managed Service) and Distributed Cloud Aggregator Management, any interaction with F5 systems, for example as part of the login flow sending signals back to F5 systems; (ii) for Distributed Cloud Account Protection, (a) a login POST transaction (for account takeover use case), and (b) an application/account creation transaction (for fake account opening); (iii) for Distributed Cloud Authentication Intelligence, a login POST Transaction; (iv) for Distributed Cloud Client-Side Defense, each distinct page view of an Authorized Website (i.e. a website on which Client-Side Defense JavaScript is injected); and (v) for Distributed Cloud Data Intelligence, any POST event (e.g., login, forgot password, payment, address change, create account).

7.1.2. **Grant of Right**. Subject to the terms and conditions of the Agreement, any applicable Orders, and the Service Policies, we grant you a limited, non-exclusive, non-transferable, non-sublicensable license during the Service Term to:

7.1.2.1. install and execute the Client-Side Code solely on the Authorized Website(s) and Authorized Mobile Application(s), for the sole purpose of collecting and generating Threat Data and transmitting the Threat Data to the SaaS Offerings; and

7.1.2.2. if an Order grants you the current right to access and use the Distributed Cloud Data Intelligence SaaS Offerings: (a) obtain the Licensed Threat Data and New Data (defined below) from the Distributed Cloud Data Intelligence SaaS Offerings; (b) internally use the Licensed Threat Data, New Data, and any Derived Data that is based on such Licensed Threat Data solely to determine whether fraudulent activities are occurring on the Authorized Websites or Authorized Mobile Applications; and (c) have only those

employees of Customer who are principally responsible for fraud detection access any such New Data, Derived Data and Licensed Threat Data (and any Documentation pertaining thereto) solely for the purposes of exercising the rights granted in Section 11.1.2.2(b) of these Service-Specific Terms; and, in each case solely for Customers' internal business purposes.

7.1.3. **Customer Responsibility.** You acknowledge and agree that you remain responsible for the security of the data being analyzed by the SaaS Offerings. If using the Application Traffic Insight ("**ATI**") functionality of the SaaS Offerings, you acknowledge and agree that a device identifier is not guaranteed to be unique, and F5 disclaims all liability under this Agreement in connection with your use of the ATI functionality. You will promptly inform us of any material Derived Data.

7.1.4. **Additional Terms Applicable to Data.**

7.1.4.1. **Threat Data**. Notwithstanding anything to the contrary set forth in the Agreement, we will have the right to collect, generate and analyze Threat Data, and we own and retain all right, title and interest worldwide in and to the Threat Data, and all intellectual property rights therein or related thereto. Threat Data does not include Customer Data.

7.1.4.2. **New Data.** Certain of the SaaS Offerings allow you to receive data from us that we own or license from a third party, or that we create through proprietary analysis and modeling of Threat Data and/or Customer Data alone or in combination with other data, such a risk score, intelligence about a threat from some source other than Customer Data, or substantiation of any of the foregoing (the "New Data"). New Data does not include Customer Data.

7.1.4.3. **Ownership of and Restrictions on use of Data.** As between you and us, we own and retain all rights, title and interest in and to the New Data, Threat Data, and Derived Data, and you hereby assign to us any right, title and interest you may have or acquire in any New Data, Threat Data and Derived Data. New Data, Threat Data and Derived Data are F5's Confidential Information. You will use New Data, Licensed Threat Data, and Derived Data only for your lawful, internal cybersecurity analysis/auditing purposes in accordance with this Agreement. You are responsible for proper security of any New Data, Licensed Threat Data, and Derived Data you receive or possess. Unless prohibited by law, you will promptly inform us of any request from a third party to exercise any purported rights with respect to the New Data, Threat Data, or Derived Data.

7.1.4.4. **Obligations on Termination**. Upon expiration of the Service Term, you will immediately: (i) discontinue use of the New Data, Licensed Threat Data and Derived Data and any Documentation pertaining thereto; (ii) return to F5, or at F5's written request destroy, all tangible materials containing, reflecting, or incorporating the New Data, Licensed Threat Data or Derived Data or any Documentation pertaining thereto; (iii) permanently erase all electronic versions of the foregoing materials from all systems you directly or indirectly control; and (iv) execute and deliver to F5, upon request, written certification of your compliance with the foregoing.

7.1.5. **Demonstration License**. In addition to the rights you grant to us to use the Customer Data in the Agreement, you hereby grant us the right and license to use the Customer Data to demonstrate to you features and functionality of additional products and services offered by us.

7.1.6. **Covenant.** Customer, on behalf of itself, its affiliates, and their successors and assigns, hereby irrevocably covenants in perpetuity not to sue F5, its affiliates, their successors and assigns, direct or indirect customers, users, licensees, service providers, distributors, retailers, or direct and indirect suppliers (collectively, "Released Parties") for infringement of any now existing or hereafter acquired patents with respect to the SaaS Offerings (or any software, services, products now existing or hereafter developed that is similar to, a replacement for or contains any functionality of any of the foregoing that is made, used, sold, offered for sale, imported or otherwise exploited by any of the Released Parties).

7.1.7. **Service Level Agreement.** During the Service Term and provided that you are compliant with the Agreement and any Service-Specific Terms, we will use commercially reasonable efforts to provide the applicable SaaS Offerings in accordance with the Service Level Agreement. The terms of this Section 11.1.7 apply solely where your access to the SaaS Offerings will be remote (i.e., all software is hosted by us on our own servers or by our third party

hosting services providers) and not where you have installed Software on physical servers or virtual machines owned or operated by you, or where your access is via Appliances delivered by us to you.

7.1.8. **Appliances**. If your access to the SaaS Offerings involves Appliances, you may order Appliances from us by submitting an Order to us. Each such Order will include, at a minimum, (i) Appliance unit quantity; (ii) shipping destination; (iii) delivery date; and (iv) other instructions or requirements pertinent to the Order. To facilitate our production schedule, all such Orders will be submitted at least 10 business days in advance of the scheduled shipping date. For the sake of convenience only, you may use your standard purchase order form for all such Orders; provided, however, that the Agreement will exclusively govern and control the ordering of Appliances from us and the use of the Software installed thereon, and any additional or contradictory terms and conditions contained on any standard purchase order form of yours will be of no effect. We will use commercially reasonable efforts to ship Appliances on or before the delivery date specified in the applicable Order (the "**Delivery Date**"). If we cannot ship Appliances by the Delivery Date, we will (i) notify you of the delay as soon as practicable; and (ii) ship the Appliances as soon as practicable. All shipments of Appliances to you will be EXW our shipping site (Incoterms 2010). You will be responsible for all costs associated with shipping, handling, and delivery.

7.1.9. **Restrictions**. Customer will not (and will not authorize or permit any third party to): (a) attempt to reverse engineer the New Data or Threat Data or any portion thereof, or otherwise attempt to derive any processes, techniques, methods, specifications, protocols, algorithms, interfaces, data structures, or other information used to collect or generate any New Data or Threat Data; (b) copy, modify or otherwise prepare derivative works of any Documentation pertaining to any of the Threat Data ; (c) rent, lease, lend, sell, sublicense, assign, distribute, publish, transfer or otherwise make available any New Data, Threat Data, or Derived Data, or Documentation pertaining thereto, or any portion thereof, to any third party, including on or in connection with the Internet or any time-sharing, service bureau, software as a service, cloud or other technology or service or otherwise use any New Data, Threat Data, or Derived Data, or Documentation pertaining thereto other than as expressly allowed under these Service-Specific Terms (d) use the New Data, Threat Data, or Derived Data, or any Documentation pertaining thereto (or any information obtained or derived from any of the foregoing) for the development, provision or use of a competing service or product; (e) externally disclose benchmarking or competitive analysis of any of the New Data, Threat Data, or Derived Data, or Documentation pertaining thereto; (f) use the New Data, Threat Data or Derived Data in violation of any applicable law or regulation or (g) allow any person (other than its employees who are principally responsible for fraud detection for the Authorized Websites and Authorized Mobile Applications) to access or use the New Data, Threat Data, or Derived Data, or any Documentation pertaining thereto, or any information obtained or derived therefrom.

7.1.10. Notwithstanding anything to the contrary in the Agreement, liabilities and damages arising out of the following will not be subject to any limitations on liability in the Agreement: Customer's unauthorized use of any of the Distributed Cloud Data Intelligence SaaS Offerings, Threat Data, Licensed Threat Data, Derived Data, or New Data (including without limitation the exercise of rights in excess of the license grants in Section 7.1.2 of these Service-Specific Terms), or Customer's breach of any of its obligations in Sections 7.1.3, 7.1.4.4, or 7.1.9 of these Service-Specific Terms.

**Data Protection Terms**

7.1.11. **DPA.** The DPA applies to personal data (as defined under the General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR")) that we process as part of the SaaS Offerings as detailed below.

7.1.12. **Processing Details and Security.** For details regarding the processing for the SaaS Offerings please refer to the DPA and Schedule A below. For a description of the technical and organizational security measures for the SaaS Offerings, please refer to Schedule B below.

**Schedule A – BRM SaaS Offerings**

**DETAILS OF THE DATA PROCESSING**

*Details relevant to Annex I(B) of the 2021 Standard Contractual Clauses*

Applied safeguards and restrictions specific to any special categories of data: Not applicable.

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

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: Personal data is retained during the subscription term. The data will be removed after termination, subject to a reasonable period of retention of copies made for backup and business continuity purposes.

* You may tailor the categories of personal data for the applicable SaaS Offering and change it over time, so the listed data elements may not reflect a comprehensive list of categories of data at all times. A comprehensive listing of categories of data will be provided via the dashboard accessible within your Account through the Portal, or otherwise made available to you by us upon request.

**Distributed Cloud Bot Defence (Managed Service) & Distributed Cloud Aggregator Management**

Subject matter, nature and purpose of processing, and details of processing operations: This SaaS Offering assesses the security/fraud risk of interactions with your online properties. It can be configured to block or simply flag suspected security/fraud risks.

Term/Duration of Processing*:* As set forth in the Agreement.

Categories of Data Subjects: Individuals who interact with your protected web and/or mobile properties.

*Categories of Data: Internet Protocol (IP) addresses, Android IDs, data about the interactions between the user (and their browser or device) and the online property; and other technical data about the browser or device that may be used to screen for malicious content, which may be collected through JavaScript, mobile software development kits (SDKs) and other technical means.

Special Categories of Data (if any): Not applicable.

**Application Traffic Insight**

Subject matter, nature and purpose of processing, and details of processing operations: This SaaS Offering assigns unique identifiers to devices that visit your online properties.

Term/Duration of Processing: As set forth in the Agreement.

Categories of Data Subjects: Individuals who interact with your protected web and/or mobile properties.

*Categories of Data: Internet Protocol (IP) addresses, fuzzy Identifiers (generated from IP addresses, User Agent strings, and select telemetry data), device identifiers (pseudo-randomly generated values), data about the user's browser or device, and data about the user's interaction with the browser or device, which may be collected through JavaScript and other technical means.

Special Categories of Data (if any): Not applicable.

**Distributed Cloud Authentication Intelligence**

Subject matter, nature and purpose of processing, and details of processing operations: This SaaS Offering helps identify returning, known users of your online property to avoid unnecessary requirements that they re-authenticate themselves.

Term/Duration of Processing*:* As set forth in the Agreement.

Categories of Data Subjects: Individuals who interact with your protected web and/or mobile properties.

*Categories of Data: Internet Protocol (IP) addresses, Fuzzy Identifiers (generated from IP addresses, User Agent strings, and select telemetry data), device identifiers (pseudo-randomly generated values), Account identifier (i.e., usernames, hashed

usernames), technical data about the user's browser or device, and data about the user's interaction with the browser or device, which may be collected through JavaScript and other technical means.

Special Categories of Data (if any): Not applicable.

**Distributed Cloud Account Protection & Distributed Cloud Data Intelligence**

Subject matter, nature and purpose of processing, and details of processing operations: This SaaS Offering provides a converged solution for application security and fraud mitigation.

Categories of Data Subjects: Individuals who interact with your protected web and/or mobile properties.

*Categories of Data: Internet Protocol (IP) addresses, Account identifier (i.e., usernames, hashed usernames), technical data about the user's browser or device, and data about the user's interaction with the browser or device, which may be collected through JavaScript and other technical means.

Special Categories of Data (if any): Not applicable.

**Distributed Cloud Client-Side Defense**

Subject matter, nature and purpose of processing, and details of processing operations: This SaaS Offering identifies malicious assets that may exfiltrate Customer's data.

Term/Duration of Processing*:* As set forth in the Agreement.

Categories of Data Subjects: Individuals who interact with your Authorized Website(s).

Categories of Data: Internet Protocol (IP) addresses, information regarding how assets of a webpage, such as JavaScript assets, are interacting with objects in a webpage and/or sending data to different end-points.

Special Categories of Data (if any): Not applicable.

**Schedule B – BRM SaaS Offerings**

**TECHNICAL AND ORGANISATIONAL SECURITY MEASURES**

*Annex II of the 2021 Standard Contractual Clauses*

We will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of your Personal Data, as described in the controls included in the following:

Service Organization Control 2 Report designed to meet the applicable criteria for the security, availability and confidentiality principles set forth in TSP Section 100A, Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy by the American Institute of Certified Public Accountants.

An Attestation of Compliance Report demonstrating compliance with applicable requirements of the Payment Card Industry – Data Security Standard version 4.0.

We may replace or modify the measures described above so long as the overall security of the SaaS Offerings is not materially lowered during a subscription term.

Subprocessors will maintain commercially reasonable security through measures that may differ from those set forth above.

**8. Terms Applicable to the following SaaS Offerings: Distributed Cloud Bot Defense (Self Service)**

**Operational Terms.**

8.1.1. **Additional Definitions.**

**"Distributed Cloud Bot Defense (Self Service) Service"** means the automated threat protection service delivered through an API.

**"Client-Side Code**" means any code, program or other software provided by F5 to Customer, such as Java Script software and SDKs, that Customer may deploy on a Covered Application to collect or generate Threat Data.

**"Covered Application"** means an application that has been enabled to make use of the Distributed Cloud Bot Defense (Self Service) Service by collecting and sending client telemetry data to the Distributed Cloud Bot Defense (Self Service) Service by means of an API call.

**"Excessive Use"** means your usage of the Distributed Cloud Bot Defense (Self Service) Service in excess of the applicable Usage Metrics, as measured by us.

**"Threat Data**" means, individually and collectively, indications of compromise, telemetry, behavioral information, device information, network information, data relating to attacks and attack tools, attack credentials and other information relating to the provision, use and performance of various aspects of the Distributed Cloud Bot Defense (Self Service) Service and any related services, systems and technologies, including any numeric or logical values generated by the Distributed Cloud Bot Defense (Self Service) Service and any contextual information associated with any such values (e.g., any description or the meaning of any such values). Threat Data does not include information that identifies a natural person.

**"Transaction"** means any interaction with F5 systems, for example as part of the login flow sending signals back to F5 systems.

**"SOC"** means the F5 security operations center.

8.1.2. **Grant of Right**. Subject to the terms and conditions of the Agreement, any applicable Orders, and the Service Policies, we grant you a limited, non-exclusive, non-transferable, non-sublicensable license during the Service Term to:

8.1.2.1. install and execute the Client-Side Code solely on a Covered Application, for the sole purpose of collecting and generating Threat Data and transmitting the Threat Data to the Distributed Cloud Bot Defense (Self Service) Service; and

8.1.2.2. if an Order grants you the current right to access and use the Distributed Cloud Bot Defense (Self Service) Service: (a) obtain the New Data (defined below) from the Distributed Cloud Bot Defense (Self Service) Service; (b) internally use the New Data solely to determine whether fraudulent activities are occurring on a Covered Application; and (c) have only those employees of Customer who are principally responsible for fraud detection access any such New Data solely for the purposes of exercising the rights granted in Section 12.1.2.2(b) of these Service-Specific Terms; and, in each case solely for Customers' internal business purposes.

8.1.3. **Additional Terms Applicable to Data.**

8.1.3.1. **Threat Data**. Notwithstanding anything to the contrary set forth in the Agreement, we will have the right to collect, generate and analyze Threat Data, and we own and retain all right, title and interest worldwide in and to the Threat Data, and all intellectual property rights therein or related thereto. Threat Data does not include Customer Data.

8.1.3.2. **New Data.** Certain of the SaaS Offerings allow you to receive data from us that we own or license from a third party, or that we create through proprietary analysis and modeling of Threat Data and/or Customer Data alone or in combination with other data, such a risk score, intelligence about a threat from some source other than Customer Data, or substantiation of any of the foregoing (the "**New Data**"). New Data does not include Customer Data.

8.1.3.3. **Ownership of and Restrictions on use of Data.** As between you and us, we own and retain all rights, title and interest in and to the New Data, and Threat Data, and you hereby assign to us any right, title and interest you may have or acquire in any New Data and Threat Data. New Data, and Threat Data are F5's Confidential Information. You will use New Data only for your lawful, internal cybersecurity analysis/auditing purposes in accordance with this Agreement. You are responsible for proper security of any New Data you receive or possess. Unless prohibited by law, you will promptly inform us of any request from a third party to exercise any purported rights with respect to the New Data.

8.1.3.4. **Obligations on Termination**. Upon expiration of the Service Term, you will immediately: (i) discontinue use of the New Data; (ii) return to F5, or at F5's written request destroy, all tangible materials containing, reflecting, or incorporating the New Data or any Documentation pertaining thereto; (iii) permanently erase all electronic versions of the foregoing materials from all systems you directly or indirectly control; and (iv) execute and deliver to F5, upon request, written certification of your compliance with the foregoing.

8.1.4. **Restrictions**. Customer will not (and will not authorize or permit any third party to): (a) attempt to reverse engineer the New Data or Threat Data or any portion thereof, or otherwise attempt to derive any processes, techniques, methods, specifications, protocols, algorithms, interfaces, data structures, or other information used to collect or generate any New Data or Threat Data; (b) rent, lease, lend, sell, sublicense, assign, distribute, publish, transfer or otherwise make available any New Data, Threat Data, or Documentation pertaining thereto, or any portion thereof, to any third party, including on or in connection with the Internet or any time-sharing, service bureau, software as a service, cloud or other technology or service or otherwise use any New Data other than as expressly allowed under these Service-Specific Terms; (c) use the New Data or the Documentation pertaining thereto (or any information obtained or derived from the New Data or such Documentation) for the development, provision or use of a competing service or product; (d) externally disclose benchmarking or competitive analysis of any of the New Data or Documentation pertaining thereto; (e) use the New Data in violation of any applicable law or regulation; or (f) allow any person (other than its employees who are principally responsible for fraud detection for the Covered Application to access or use the New Data or any Documentation pertaining thereto, or any information obtained or derived therefrom.

8.1.5. **Excessive Use**. We may monitor your use of the Distributed Cloud Bot Defense (Self Service) Service for Excessive Use. If your usage of the Distributed Cloud Bot Defense (Self Service) Service is deemed Excessive Use, as measured by us, you will (i) negotiate in good faith with us to increase the capacity of the Distributed Cloud Bot Defense (Self Service) Service to cover such Excessive Use, and (ii) place additional orders for the Distributed Cloud Bot Defense (Self Service) Service to remedy the Excessive Use

8.1.6. **Service Level Agreement**. During the Service Term and provided that you are compliant with the Agreement and any Service-Specific Terms, we will use commercially reasonable efforts to provide the Distributed Cloud Bot Defense (Self Service) Service in accordance with the Service Level Agreement for Distributed Cloud Bot Defense (Self Service) (excluding any Root Cause Analysis).

8.1.7. **Service Tier Descriptions.**

8.1.7.1. Distributed Cloud Bot Defense (Self Service) Service includes:

(i) SOC support by phone, chat and email to maintain security policies in support of your Covered Applications, including onboarding and configuration of the Distributed Cloud Bot Defense (Self Service) Service.

8.1.8. Notwithstanding anything to the contrary in the Agreement, liabilities and damages arising out of the following will not be subject to any limitations on liability in the Agreement: Customer's unauthorized use of the Distributed Cloud Bot Defense (Self Service) Service, Threat Data, or New Data (including without limitation the exercise of rights in excess of the license grants in Section 12.1.2 of these Service-Specific Terms), or Customer's breach of any of its obligations in Sections 12.1.3.4, or 12.1.4 of these Service-Specific Terms.

**Data Protection Terms.**

8.1.9. DPA. The DPA applies to the any personal data (as defined under the General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR")) that we process on your behalf through the Integrated Bot Defence Services as detailed below.

8.1.11. Processing Details and Security. For details regarding the processing please refer to the DPA and Schedule A below. For a description of the technical and organizational security measures for the Distributed Cloud Bot Defense (Self Service) Service, please refer to Schedule B below.

**Schedule A - Distributed Cloud Bot Defense (Self Service) Service**

**DETAILS OF THE DATA PROCESSING**

*Details relevant to Annex I(B) of the 2021 Standard Contractual Clauses*

Subject Matter, Nature and Purpose of Processing, and details of processing operations: Provision of the Distributed Cloud Bot Defense (Self Service) Service, as described herein.

Term/Duration of Processing: As set forth in the Agreement.

Categories of Data Subjects: Visitors to your Internet-facing websites and mobile applications protected by the Distributed Cloud Bot Defense (Self Service) Service

Categories of Data: Internet Protocol (IP) addresses; Distributed Cloud Bot Defense (Self Service) Service identifiers (pseudo-randomly generated values); information from interactions between the user (and their browser or device) and the online property; and other technical data about the browser or device that may be used to screen for malicious activity.
Special Categories of Data (if any): Not applicable.

Applied safeguards and restrictions specific to any special categories of data: Not applicable.

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

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: Personal data is retained during the subscription term. The data will be removed after termination, subject to a reasonable period of retention of copies made for backup and business continuity purposes.

**Schedule B - Distributed Cloud Bot Defense (Self Service) Service**

**TECHNICAL AND ORGANISATION SECURITY MEASURES**

*Annex II of the 2021 Standard Contractual Clauses*

We will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of your Personal Data, as described in the controls included in the following:

Service Organization Control 2 Report designed to meet the applicable criteria for the security, availability and confidentiality principles set forth in TSP Section 100A, Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy by the American Institute of Certified Public Accountants.

An Attestation of Compliance Report demonstrating compliance with applicable requirements of the Payment Card Industry – Data Security Standard version 4.0.

We may replace or modify the measures described above so long as the overall security of the Distributed Cloud Bot Defense (Self Service) Service is not materially lowered during a subscription term.

Subprocessors will maintain commercially reasonable security through measures that may differ from those set forth above.

**9. Professional Services**

**Additional Definitions.**

"**Professional Services**" means implementation and configuration services provided by us in connection with the F5 Services.

"**Statement of Work**" means a document that describes Professional Services purchased by you. Each Statement of Work incorporates the terms of this Agreement by reference, or such other agreement between us and you governing the provision of Professional Services.

**Provision of Professional Services; Fees.**

Subject to these Service-Specific Terms, you may order Professional Services from us, and we will provide the Professional Services as set forth in such Order. The scope, timeline and tasks of the parties with respect to the Professional Services shall be as specified in the applicable Order or in any mutually executed Statement of Work. Unless otherwise set forth in the Order or Statement of Work for Professional Services, as applicable, the fees for such Professional Services shall be based on our then-current rates for such Professional Services. You will pay the fees for such Professional Services as set forth in the applicable Order.

**Expenses.**

Unless otherwise specified in the applicable Statement or Work (or if no Statement of Work, agreed to in writing by the parties), upon invoice from us, you will reimburse us for all pre-approved, reasonable expenses incurred by us while performing Professional Services. We will include reasonably detailed documentation of all such expenses with each related invoice.

**10. Terms Applicable to the following SaaS Offerings (collectively "XC SaaS Offerings"): Distributed Cloud Mesh, Distributed Cloud App Stack, Distributed Cloud DDoS, Distributed Cloud WAF, Distributed Cloud API Security, Distributed Cloud Network Connect, Distributed Cloud Load Balancer, Distributed Cloud App Connect, Distributed Cloud DNS, Distributed Cloud DNS Load Balancer, Distributed Cloud Synthetic Monitoring, and Distributed Cloud CDN.**

**Usage Metrics.**

For purposes of measuring use of the applicable Distributed Cloud SaaS Offerings, the following measurement methodologies will be applied:

10.1.1. Distributed Cloud Load Balancers – The maximum number of active Load Balancers deployed during a given month during the Service Term.

10.1.2. Distribute Cloud Web Application Firewall ("WAF") – The maximum number of WAF enabled Distributed Cloud Load Balancers deployed during a given month during the Service Term.

10.1.3. Distributed Cloud DNS.

10.1.3.1. Distributed Cloud DNS Zones - The maximum number of active DNS Zones deployed during a given month during the Service Term. A DNS Zone is active if it has been used for more than 24 hours during the given month.

10.1.3.2. Distributed Cloud DNS Load Balancer Record - The maximum number of Load Balancer Records configured during a given month during the Service Term

10.1.3.3. Distributed Cloud DNS Health Check - The number of Load Balancer Health Checks performed during a given month during the Service Term.

10.1.4. Distributed Cloud Mesh VIP (BYO) or Distributed Cloud Mesh VIP (Anycast) - The total number of the applicable active VIPs deployed during a given month during the Service Term, determined by dividing the total number of hours each VIP is deployed per month by the number of hours per month, then rounding up to the nearest integer.

10.1.5. Distributed Cloud API Security - The sum of API requests during a given month during the Service Term.

10.1.6. Distributed Cloud Mesh Rate Limiting - The sum of Good Requests during a given month during the Service Term. "Good Request" is a request which has not been identified as a request generated either by a bad actor or one which is a violation of the security controls such as known patterns through signature matches or behavioral observation.

10.1.7. Distributed Cloud DDoS

10.1.7.1. DDoS Mitigation Tunnel - The maximum number of tunnels deployed during a given month during the Service Term.

10.1.7.2. DDOS Mitigation Router Monitoring – The maximum number of routers enabled for Router Monitoring during a given month during the Service Term.

10.1.7.3. DDOS Mitigation ACL Rules - The maximum number of DDOS Mitigation ACL Rules deployed during a given month during the Service Term.

10.1.8. Distributed Cloud CDN

10.1.8.1. Distributed Cloud CDN Bandwidth - The sum of data transferred to the Internet during a given month during the Service Term.

10.1.8.2. Distributed Cloud CDN HTTP(s) Requests - The sum of HTTP(s) requests during a given month during the Service Term.

10.1.9. Distributed Cloud Mesh Nodes or Distributed Cloud Stack Nodes - The total number of applicable active nodes deployed during a given month during the Service Term, determined by the sum of the number of hours each node has been deployed / number of hours per month, rounded up to the nearest integer.

10.1.10. Distributed Cloud App Stack Traffic - The sum of the data generated by node to ADN during a given month during the Service Term.

10.1.11. Distributed Cloud Synthetic Monitoring – The number of executions is the sum of individual times a monitor has been run across all configured regions during a given month during the Service Term.

**Operational Terms For: Distributed Cloud Mesh, Distributed Cloud App Stack, Distributed Cloud API Security, Distributed Cloud Network Connect, Distributed Cloud Load Balancer, Distributed Cloud App Connect, Distributed Cloud DNS, Distributed Cloud DNS Load Balancer, Distributed Cloud Synthetic Monitoring, and Distributed Cloud CDN:**

**10.1.12. Additional Definitions.**

**"Authorized Devices"** means the number of computer devices owned or controlled by you on which the Desktop Software is authorized to be installed, as specified in the applicable Order and/or any applicable Usage Metrics set forth in such Order.

**"Authorized Machines"** means the number of physical servers or virtual machines owned or operated by you on which the Machine Software is authorized to be installed, as specified in the applicable Order and/or any applicable Usage Metrics set forth in such Order. Authorized Machines may be located in the data centers of your hosting service providers, so long as the Authorized Machines are solely under your control. If you have purchased or licensed Hardware from us under this Agreement, such Hardware shall be deemed an "Authorized Machine" as used in this Agreement.

**"Desktop Software"** means F5's proprietary client software programs set forth in an Order that are made available to you hereunder, in executable code form, for installation on Authorized Devices, and any and all modified, updated, or enhanced versions thereof that are provided to you under this Agreement.

**"Machine Software"** means the proprietary F5 server software programs set forth in the applicable Order that are made available to you hereunder, in executable code form, either (a) for installation and use on Authorized Machines, or (b) pre-installed on Hardware; and any and all modified, updated, or enhanced versions of the programs described in clause (a) and (b) that are provided to you under this Agreement.

**"Hardware"** means the server hardware device onto which we have pre-installed Machine Software, licensed by you as part of, or purchased by you hereunder for use in connection with, the SaaS Offerings, as set forth in your Order and as further described in the Service Policies.

**"SDK"** means any software development kits provided to you by us under this Agreement, as set forth in your Order and as further described in the Service Policies.

**"Software"** means the Desktop Software and Machine Software.

10.1.13. Access Rights.

10.1.13.1. **SaaS Offerings.** Subject to the terms and conditions of the Agreement, any applicable Orders, and the Service Policies, we grant you a limited, revocable, non-exclusive, non-transferable, non-sublicensable right to (a) permit Users to access and use the SaaS Offerings, solely through the Customer website portal specified in an Order; and (b) permit End Users to access and use the Customer Dashboard, solely through the Customer website portal specified in an Order, each of which in accordance with the terms of the Agreement and solely in connection with your internal business purposes during the applicable Service Term and subject to any Usage Metrics.

10.1.13.2. **Software.** Subject to your compliance with the terms of the Agreement (including the Service Policies), we grant you, during the applicable Service Term, a limited, revocable, non-exclusive, non-transferable, non-sublicensable license:

(a) if you have licensed the Machine Software for installation on Authorized Machines, as specified in the applicable Order, to install and execute the Machine Software on

Authorized Machines in object code form only, solely to access and use the SaaS Offerings, using the Machine Software;

(b) to permit Users to install, execute and use the Desktop Software on Authorized Devices, in executable code form only, solely to access and use the SaaS Offerings, using the Desktop Software; and

(c) in each case, solely for your internal business and in accordance with the Agreement and the applicable Documentation, and subject to any Usage Metrics.

10.1.13.3. **Hardware.** Subject to your compliance with the terms of the Agreement (including the Service Policies), we grant you, during the applicable Service Term, a limited, personal, non-sublicensable non-exclusive, non-transferable, license:

(d) if you have obtained the rights to use the Hardware as part of a subscription to use the SaaS Offerings, to access and use the Hardware solely internally in connection with your use of the SaaS Offerings;

(e) if you have obtained the Hardware as part of, or purchased the Hardware from us in connection with, a subscription or license, to execute and use the Machine Software pre-installed on the Hardware, in object code form only, solely to access and use the SaaS Offerings, over the Internet; and

(f) in each case, solely for your internal business and in accordance with the Agreement and the applicable Documentation, and subject to any Usage Metrics.

10.1.14. **Third-Party Access to Distributed Cloud Mesh.** As part of the SaaS Offerings, you may have the opportunity to grant any third-party entity or website the ability to access your Account. Should you elect to do so, you acknowledge and agree that we cannot be responsible for damages, harm, or losses that may arise from the third-party's access to your Account.

10.1.15. Terms Applicable to Hardware.

10.1.15.1. **Purchase Price for Hardware.** The purchase price for the Hardware will be as set forth on the applicable Order and due and payable by you within thirty (30) days following the date of the Order unless otherwise set forth therein. Unless otherwise stated in the applicable Order, the purchase price for the Hardware is exclusive of, and you shall be responsible for, all fees and costs for delivery, packaging, packing, shipping, carriage, and/or insurance.

10.1.15.2. **Use Restriction and Shipment.** Except as expressly set forth in this Agreement, you will not (and will not allow any third party to) disassemble the Hardware. We will use commercially reasonable efforts to ship the Hardware on or before the quoted shipment date to you or our carrier agent at our facility or the facility of our contract manufacturer, at which time risk of loss and, if you have purchased the Volterra hereunder, title, will pass to you. In the absence of specific shipping instructions from you, we will choose the method of shipment in its discretion. You will pay all freight, insurance, and other shipping expenses. We will notify you of any anticipated or actual delay in delivery. Notwithstanding the foregoing, we shall not be liable for any liability, loss, damage, cost or expense incurred by you or any other person or entity arising form or related to any failure by us to complete deliver of the Hardware. The Hardware will be deemed accepted upon delivery to you.

10.1.15.3. **Ownership.** You agree that the Hardware shall remain the personal property of F5 and you shall have no right, title, or interest therein. You shall keep the Hardware free from all liens, attachments, encumbrances or judicial processes and shall not act, or fail to act, in any manner inconsistent with our title including, but not limited to, not transferring, selling, assigning, sublicensing, pledging, or otherwise disposing, encumbering, or suffering a lien or encumbrance upon or against any interest in the Hardware without our prior written consent. Notwithstanding the foregoing, if you have

purchased the Hardware from us hereunder, you shall retain title to such Hardware, subject to our intellectual property rights in and to the SaaS Offerings, including, without limitation, any Software embedded or installed on the Hardware.

10.1.15.4. **Limited Hardware Warranty.** If you have purchased Hardware under this Agreement, we warrant that the Hardware will, for a period of three (3) years from the date of delivery of the Hardware to you (the "Warranty Period"), be free from defects in material and workmanship under normal use. As your sole and exclusive remedy, and our sole and exclusive liability, for any breach of this warranty, we shall, at our option and expense, (a) repair or replace the non-conforming Hardware, or (b) issue you a credit or refund in the amount of the purchase price for such Hardware; provided that (i) we are notified in writing by you within thirty (30) days after discovery of such failure; (ii) you obtain an RMA from us prior to returning any defective Hardware to us; (iii) the defective Hardware is returned to the location specified by us; (iv) the defective Hardware is received by us not later than four (4) weeks following the last day of the Warranty Period; and (v) our examination of such Hardware discloses that such failures have not been caused by improper installation by or application, repair, alteration, accident or negligence. Any such repair, replacement or return of the Hardware provided to you will not extend the original warranty. The foregoing limited warranty extends only to the original Customer who purchases the Hardware under this Agreement (and not to any subsequent purchasers or third parties). The foregoing limited warranties shall be null and void to the extent the Hardware: (1) has been altered or serviced, except by us or one of our authorized service providers; (2) has not been installed, operated, repaired, or maintained in accordance with our instructions; (3) is used for an unintended purpose, is used other than in accordance with its published documentation or specifications, or is otherwise used in breach of this Agreement; (4) fails to conform with this warranty as a result of its use with any third-party hardware or software; (5) has been subjected to abnormal physical or electrical stress, misuse, negligence or accident; or (6) has been damaged or rendered defective by the use of parts not manufactured or sold by us.

10.1.15.5. **Warranty Returns.** To request a return materials authorization (RMA) under the warranty provided above, please file a support ticket through the applicable Customer Dashboard and specify "Return Materials Authorization (RMA) required" on such support ticket. If your RMA request is approved, we will email you an RMA number. You will be responsible for shipping the defective unit back to us. We will troubleshoot and attempt to fix the defective unit. If the defective unit can be fixed, we will fix it and send you the repaired unit. If we cannot fix the defective unit, we will send you a replacement unit. The standard warranty covers parts only and does not cover labor nor on-site support.

10.1.15.6. **Refund Requests.** If you are dissatisfied with your Hardware purchase for any reason, please contact (a) us if you purchased from us directly, or (b) the authorized reseller from whom you purchased the Hardware.

10.1.15.7. **Shipment Preparation.** You must return units in their entirety, including all power supplies, antennas, and other components along with the original product box. Please use the original shipping carton and packaging material. If this is not possible, use another shipping carton with padding to protect the units from damage during shipping, and remove ALL inappropriate and/or inapplicable label(s). You MUST NOT ship a product without a carton. You will be charged for a product that is damaged due to insufficient packaging. If we approve your RMA request, you will receive a confirmation email containing an RMA number within two business days. The address to which the product should be sent will also be included in that email. Once you have received your RMA number from us via email, write this RMA number in large letters on the exterior of the shipping carton. Shipments to us without an RMA approval will not be processed. We will provide a pre-paid return shipping label for warranty replacement return shipments.

10.1.15.8. **Effect of Termination.** Upon termination of the Agreement, and without limiting your rights and obligations therein, if you have licensed the Hardware as part of the F5 Services, you shall promptly return to us, in good working order (reasonable and normal wear and tear excepted), at our cost using our designated shipping account, all units of Hardware. You must use F5 shipping

containers to return the Hardware units. If you have purchased the Hardware hereunder, upon any termination or expiration of this Agreement, you shall immediately remove the Software (including any updates) from the Hardware, and destroy any copies thereof in your possession or control.

**Operational Terms for: Distributed Cloud DDoS and Distributed Cloud WAF**

10.1.16. **Additional Definitions.** Unless otherwise defined in these Service-Specific Terms, the following definitions apply:

10.1.16.1. "**95th Percentile Calculated Bandwidth**" means your bandwidth calculated as: collecting 5-minute samples over a calendar month based on traffic that is transmitted or received between the F5 Distributed Cloud Network and your network, sorting the samples from largest to smallest, discarding the top (highest) 5 percent of samples, and selecting the remaining highest single sample. The selected sample determines the bandwidth at the 95th percentile value.

10.1.16.2. **"DDoS"** means distributed denial of service.

10.1.16.3. **"Excessive Use"** of a Distributed Cloud SaaS Offering shall have the meaning set forth in the applicable Service-Specific Term.

10.1.16.4. **"F5 Distributed Cloud Network"** means the IP network owned or operated by us related to the Distributed Cloud SaaS Offerings and the system(s) (servers, and associated software) deployed by us for the delivery of the Distributed Cloud SaaS Offerings. The F5 Distributed Cloud Network does not include customer-side web-based user interfaces, zone/data transfer mechanisms, customer-side web servers, application programming interfaces, or other customer accessible data manipulation software, Internet connectivity provided by third parties, the telecommunications means between the servers, nor the Internet routes between servers.

10.1.16.5. **"Distributed Cloud SaaS Offerings"** means the Distributed Cloud DDoS Protection Service; ; and the **Distributed Cloud** Web Application Firewall Service.

10.1.16.6. **"Distributed Cloud DDoS Protection Service"** means the distributed denial of service protection service delivered through the F5 Distributed Cloud cloud-based platform. The Distributed Cloud DDoS Protection Service is also governed by the Distributed Cloud DDoS Protection Service-Specific Terms.

10.1.16.7. **"Distributed Cloud Web Application Firewall Service"** means the web application firewall service delivered through the F5 Distributed Cloud cloud-based platform. The Distributed Cloud Web Application Firewall Service is also governed by the Distributed Cloud Web Application Firewall Service-Specific Terms.

10.1.16.8. **"SOC"** means F5's security operations center.

**10.1.17. Additional Terms.**

10.1.17.1. **Excessive Use**. We may monitor your use of the Distributed Cloud SaaS Offerings for Excessive Use. If your usage of the Distributed Cloud SaaS Offerings is deemed Excessive Use, as measured by us, you will (i) negotiate in good faith with us to increase the capacity of such Distributed Cloud SaaS Offerings to cover such Excessive Use, and (ii) place additional orders for the applicable Distributed Cloud SaaS Offering to remedy the Excessive Use.

10.1.17.2. **Service Term – Subscription Start Date**. The Service Term for the Distributed Cloud SaaS Offerings shall start on the Subscription Start Date. "Subscription Start Date" shall mean the start date set forth in the applicable Order that has been accepted by F5;

10.1.17.3. **Service Term – Under Attack**. Notwithstanding the foregoing, if you order Distributed Cloud SaaS Offerings while under a DDoS attack, the Subscription Start Date shall start on the date that you have accepted this Agreement for the applicable Distributed Cloud SaaS Offering. You hereby acknowledge and agree that you are obligated to promptly place an Order for such Distributed Cloud SaaS Offering with us or an Authorized Distribution Partner, as applicable, and pay applicable fees for such Distributed Cloud SaaS Offering.

10.1.17.4. **Security**. During any Service Term, we shall implement a security program for the applicable Distributed Cloud SaaS Offering that is designed to comply with the Payment Card Industry Data Security Standard (PCI-DSS) or any similar industry security standard. Upon your written request, which shall not be made more than once in any twelve (12) month period, we shall provide you a PCI-DSS, or other similar security standard, attestation of compliance, or similar certification of compliance, applicable to the Distributed Cloud SaaS Offerings provided hereunder.

10.1.17.5. **New Data**. Certain Distributed Cloud SaaS Offerings allow you to receive data from us that we own or license from a third party, or that we create through proprietary analysis and modeling of Customer Data alone or in combination with other data, such as risk score, intelligence about a threat from some source other than Customer Data, or substantiation of either of the foregoing (collectively, "New Data"). New Data does not include Customer Data. As between you and us, we own and retain all rights, title and interest in and to the New Data, and you may use New Data only for your lawful, internal cybersecurity analysis/auditing purposes in accordance with this Agreement. You are responsible for proper security of any New Data you receive. Unless prohibited by law, you will promptly inform us of any request from a third party to exercise any purported rights with respect to the New Data.

10.1.18. **Distributed Cloud DDoS Protection Service Operational Terms.**

10.1.18.1. **Additional Definitions.** Unless otherwise defined in these Service-Specific Terms, the following definitions apply:

(g) "**Always Available**" means a Distributed Cloud DDoS Protection Service where all prerequisite configuration elements are established and you determine when to, and take action to, divert your traffic to the F5 Distributed Cloud Network for DDoS mitigation.

(h) "**Always On**" means a Distributed Cloud DDoS Protection Service where your applicable traffic protected from attack is continuously directed to the F5 Distributed Cloud Network for DDoS monitoring and mitigation.

(i) "**Clean Bandwidth**" means the 95$^{th}$ Percentile Calculated Bandwidth of traffic returned to, or received from, your premises after the Distributed Cloud DDoS Protection Service mitigation methods are applied.

(j) "**Data Center**" means a single physical location or a virtual construct that is used to centralize computing resources. A data center may support multiple applications, or IP Subnets. For the Distributed Cloud DDoS Protection Service, 4 (four) clean traffic return paths will be configured for each Customer Data Center (e.g., GRE tunnels).

(k) "**Router Monitoring**" means that we will monitor for Layer 3-4 DDoS events while your traffic is not running through the F5 Distributed Cloud Network. Router Monitoring requires you to appropriately configure identified routers to send flow data to us for the purpose of monitoring traffic for DDoS events. The number of your routers configured to transmit flow data to us will determine quantity of Router Monitoring objects.

(l) "**VIP**" means an IP address configuration provided to you by us which includes an IP address allocated by us to process and transmit traffic to defined origin(s) within your Data Center. The VIPs are used in a proxy deployment to enable communication from the Internet to us and then to your application within your Data Center.

10.1.18.2. **Excessive Use.** For the purpose of this Service-Specific Term, "**Excessive Use**" means your usage of the Distributed Cloud DDoS Protection Service in (a) excess of the Clean Bandwidth as measured by 95$^{th}$ Percentile Calculated Bandwidth; or (b) your configuration of Router Monitoring or Data Centers (e.g., GRE Tunnels) exceeds the quantities defined in the applicable Order.

10.1.18.3. **Additional Disclaimers and Limitations.** DISTRIBUTED CLOUD DDOS PROTECTION SERVICES PROVIDE PROTECTION ONLY IN ACCORDANCE WITH THE SPECIFICATIONS ASSOCIATED WITH THE APPLICABLE DISTRIBUTED CLOUD DDOS PROTECTION SERVICE, SUBJECT TO YOUR ORDERING AND PAYING APPLICABLE FEES FOR SUCH SAAS OFFERINGS IN ACCORDANCE WITH THE APPLICABLE PAYMENT TERMS, INCLUDING SPECIFICATIONS ON CLEAN BANDWIDTH, NUMBER OF DATA CENTERS, NUMBER OF VIPS, ROUTER MONITORING QUANTITY AND WHETHER SUCH SERVICES ARE ALWAYS ON OR ALWAYS AVAILABLE.

10.1.19. Distributed Cloud Web Application Firewall Operational Terms.

10.1.19.1. Additional Definitions.

Unless otherwise defined in these Service-Specific Terms, the following definitions apply:

(a) **Domain(s)"** means a fully-qualified domain name which, by means of a domain name system (DNS), points to a single canonical name (CNAME), a single IP address, or a single pool of distributed IP addresses.

(b) "**Load Balancer**" or "**LB**" means a reverse proxy that distributes application traffic across several servers. For the Distributed Cloud Web Application Firewall Service, this refers to HTTP Load Balancers where the Distributed Cloud Web Application Firewall Service can be enabled to selectively block HTTP/HTTPS requests that match the Distributed Cloud Web Application Firewall Service policy criteria.

10.1.19.2. **Excessive Use.** For purposes of this Service-Specific Term, "**Excessive Use**" means your usage of the **Distributed Cloud** Web Application Firewall Service (a) in excess of the bandwidth provided for in the applicable Order, as measured by us where use shall be excessive if either (i) the 95$^{th}$ Percentile Calculated Bandwidth exceeds the applicable tier defined in the Order; or (ii) you are targeted by a sustained DDoS attack whereby your application consumes more than one DDoS attack that exceeds a peak of 1.5 Gbps of attack traffic during any twelve (12) month period, unless you have an effective subscription to Distributed Cloud DDoS Protection Service covering such attack or (b) where you have provisioned a quantity of LBs for protection via the Distributed Cloud Web Application Firewall Service greater than the defined amount of LBs in the Order. You acknowledge and agree that our obligations are limited to providing the Distributed Cloud Web Application Firewall Service in the quantities identified in the Order(s) for the active Service Term(s).

10.1.19.3. **Distributed Cloud Managed Services.** The following section applies only to Managed Services offering:

(a) Distributed Cloud Managed Web Application Firewall Service. Distributed Cloud Managed Web Application Firewall Service includes:

(i) SOC support by phone, chat and email to maintain security policies in support of your covered Domain(s)(i.e. those configured in the Web Application Firewall Service associated with the Load Balancers), including periodic tuning of security policies in accordance with the results of vulnerability assessments as performed against your covered Domain(s).

(ii) Detailed analysis of your web application firewall violation logs for the purpose of tuning the security policies.

(iii) Vulnerability assessment data imported from a third party or sources provided by you.

(iv) Reporting on web application firewall violation data.

(v) Upon yours request, the SOC may also engage with you for web application firewall violation false positive reviews.

10.1.19.4. **Additional Disclaimers and Limitations.** DISTRIBUTED CLOUD WEB APPLICATION FIREWALL SERVICES PROVIDE PROTECTION FOR ONLY DOMAIN(S) ASSOCIATED WITH LOAD BALANCERS CONTRACTUALLY ASSOCIATED WITH THE DISTRIBUTED CLOUD WEB APPLICATION FIREWALL SERVICE ON THE APPLICABLE ORDER(S). IN THE EVENT THAT YOU QUALIFY FOR, PURSUANT TO OUR ELIGIBILITY CRITERIA AS MAY BE CHANGED FROM TIME TO TIME IN OUR SOLE DISCRETION, AND ELECT TO EXPORT YOUR WEB APPLICATION FIREWALL POLICIES ("**WAF POLICIES**") FROM THE DISTRIBUTED CLOUD WEB APPLICATION FIREWALL SERVICES FOR USE IN CONNECTION WITH YOUR SEPARATELY LICENSED F5 APPLICATION SECURITY MANAGER SOFTWARE ("**WAF POLICY EXPORT**"), YOU ACKNOWLEDGE AND AGREE THAT SUCH EXPORT AND USE OF THE WAF POLICIES ARE AT YOUR SOLE RISK. WE HEREBY DISCLAIM ALL LIABILITY, EXPRESS OR IMPLIED, IN CONNECTION WITH YOUR WAF POLICY EXPORT, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTIES AGAINST INFRINGEMENT OF THIRD-PARTY RIGHTS, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE (INCLUDING, WITHOUT LIMITATION, DETECTION OF DISTRIBUTED DENIAL OF SERVICE ATTACKS). YOU ACKNOWLEDGE AND AGREE THAT WE HAVE NO OBLIGATION TO PROVIDE SUPPORT TO YOU IN CONNECTION WITH SUCH WAF POLICY EXPORT.

**Service Level Agreement.**

Subject to your compliance with the Agreement and the Service Policies, we will make the SaaS Offerings available to you in accordance with the Service Level Agreement.

**Data Protection Terms**

10.1.20. **DPA.** The DPA applies to personal data (as defined under the General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR")) that we process as part of the SaaS Offerings as detailed below.

10.1.21. **Processing Details and Security.** For details regarding the processing for the SaaS Offerings please refer to the DPA and Schedule A below. For a description of the technical and organizational security measures for the SaaS Offerings, please refer to Schedule B below.

**Schedule A – XC SaaS Offerings**

**DETAILS OF THE DATA PROCESSING**

*Details relevant to Annex I(B) of the 2021 Standard Contractual Clauses*

Applied safeguards and restrictions specific to any special categories of data: Not applicable.

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

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: Personal data is retained during the subscription term. The data will be removed after termination, subject to a reasonable period of retention of copies made for backup and business continuity purposes.

Subject matter, nature and purpose of processing, and details of processing operations: Provision of the SaaS Offerings, as described herein.

Term/Duration of Processing: As set forth in the Agreement.

Categories of Data: Data relating to individuals provided to F5 via the SaaS Offerings by, or at the direction of, you or your end users, the extent of which is determined and controlled solely by you or your end users and may include but is not limited to: first and last name, billing address, title, position, employer, contact information (email, phone, physical address), connection data, localization data, credit card information, Internet Protocol (IP) addresses, network traffic data, user identifiers, passwords, API logs, cookies, account identifier (i.e., usernames, hashed usernames), and other technical data about the user's browser or device (which may, for example, be used to screen for malicious activity). Distributed Cloud Web Application Firewall Service may use information in an HTTP/HTTPS request to determine if a Distributed Cloud Web Application Firewall Service policy has been violated and mitigate that violation/request; Distributed Cloud Web Application Firewall Service will store the policy along with the data that violated the policy, however, customers may set filters to prevent certain data from being persistently stored.

Categories of Data Subjects: Data subjects include the individuals about whom data is provided to F5 via the SaaS Offerings by, or at the direction of, you or your end users, the extent of which is determined and controlled solely by you or your end users and may include but is not limited to: your customers, prospects, partners, vendors, employees, contractors, and third-party service providers.

Special Categories of Data (if any): You or your end users may, subject to the restrictions set forth in the End User Services Agreement, provide special categories of personal data to F5 via the SaaS Offerings, the extent of which is determined and controlled solely by you or your end users.

**Schedule B – XC SaaS Offerings**

**TECHNICAL AND ORGANISATION SECURITY MEASURES**

*Annex II of the 2021 Standard Contractual Clauses*

We will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of your Personal Data, as described in the controls included in the following:

Service Organization Control 2 Report designed to meet the applicable criteria for the security, availability and confidentiality principles set forth in TSP Section 100A, Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy by the American Institute of Certified Public Accountants.

An Attestation of Compliance Report demonstrating compliance with applicable requirements of the Payment Card Industry – Data Security Standard version 4.0.

We may replace or modify the measures described above so long as the overall security of the SaaS Offerings is not materially lowered during a subscription term.

Subprocessors will maintain commercially reasonable security through measures that may differ from those set forth above.

**11. Terms Applicable to the following SaaS Offering: NGINX on Azure**

**Service Level Agreement.**

Subject to your compliance with the Agreement and the Service Policies, we will make NGINX on Azure available to you in accordance with the Service Level Agreement.

**Data Protection Terms**

11.1.1. **DPA**. The DPA applies to personal data (as defined under the General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR")) that we process as part of NGINX on Azure as detailed below.

11.1.2. **Processing Details and Security**. For details regarding the processing for NGINX on Azure please refer to the DPA and Schedule A below. For a description of the technical and organizational security measures for NGINX on Azure, please refer to Schedule B below.

**Schedule A – NGINX on Azure**

**DETAILS OF THE DATA PROCESSING**

*Details relevant to Annex I(B) of the 2021 Standard Contractual Clauses*

Subject matter, nature and purpose of processing, and details of processing operations: Provision of NGINX on Azure, as described herein.

Term/Duration of Processing: As set forth in the Agreement.

Categories of Data: full name, contact details, IP address, diagnostic data, telemetry, error reports, localization data, work email, account information, and browsing information.

Categories of Data Subjects: Customer and Customer's customers.

Special Categories of Data (if any): Not Applicable

Applied safeguards and restrictions specific to any special categories of data: Not applicable.

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

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: Personal data is retained during the subscription term and for approximately seven days after termination.

**Schedule B – NGINX on Azure**

**TECHNICAL AND ORGANISATION SECURITY MEASURES**

*Annex II of the 2021 Standard Contractual Clauses*

***Information Security Program.*** **We maintain a written information security program that contains administrative, technical and physical safeguards that are appropriate to the type of information that we may receive as a result of providing Services and the need for security and confidentiality of such information. Without limiting the foregoing:**

Network configuration security.

Elimination of default system passwords and other security parameters on systems used to host or process personal data.

Functional and regularly updated anti-virus controls on systems used to host or process personal data.

Exclusive use of unique, traceable system IDs on systems used to host or process personal data.

Controls to restrict physical access controls to systems used to host or process personal data.

Logging and monitoring of access to informational processing systems, including systems that store personal data and systems hosting personal data.

Regular testing of security controls.

Creation and maintenance of an information security policy, and communication of this policy to personnel who have access to personal data at the F5 Data Centre.

***Access control to premises and facilities:*** **Technical and organizational measures to control access to premises and facilities, particularly to check authorization:**

Access control systems: issue of ID reader; magnetic card; chip card; keys.

Automatic door locking.

Security staff at data centers and key offices.

Surveillance facilities: Alarm system; CCTV monitor.

Isolation of areas containing sensitive information or equipment.

***Access control to systems*: Information system access is enabled through network domain accounts, also referred to as User IDs, user names, or accounts. Unique user IDs are issued to individuals through central registration, request, and management approval processes administered by the IT Service Desk. A password is associated with each User ID.**

***User Responsibilities:* Each user is personally responsible for all system activity associated with their assigned User IDs. Assigned User IDs and passwords may not be shared with anyone else. Password management acceptable use practices are communicated to users through company policy.**

***Password Management Standards for Applications:* Internal and external applications must integrate with existing F5 authentication systems. New applications which fail to meet company policy and standards may not be deployed for F5 use.**

***Multi-factor Authentication:* Where required by management, multi-factor authentication is required for remote access or access to sensitive systems and consoles.**

***Role based access control to data:* Requirements driven definition of the authorization scheme and access rights and logging and monitoring of access:**

Differentiated access rights: profiles; roles; transactions and objectives

Reports

***Disclosure control:* Measures to transport, transmit and communicate or store data on media (manual or electronic) and for subsequent checking:**

Encryption / funneling: VPN

Transport security

***Availability control:* Measures to assure data security (physical/logical):**

Capacity management

Backup procedures

Mirroring of hard disks (e.g., RAID technology)

Uninterruptable power supply

Remote storage

Disaster recovery plan

***Segregation control:* Measures to provide for separate processing (storage, amendment, deletion, transmission) of data for different purposes:**

"Critical" concept / limitation of use

Segregation of functions (development/testing/production). We may replace or modify the measures described above so long as the overall security of the applicable SaaS Offerings is not materially lowered during a subscription term.

Subprocessors may maintain commercially reasonable security through measures that may differ from those set forth above.

**12. Distributed Cloud (XC) Mobile App Shield**

**Usage Metrics.**

For purposes of measuring use of Distributed Cloud Mobile App Shield, the following measurement methodology will be applied: the number of unique monthly active users of each of your mobile applications protected by Distributed Cloud (XC) Mobile App Shield.

**Additional Definitions.**

12.1.1. **"Authorized Mobile Application(s)"** means the Customer's mobile application(s) being monitored by Distributed Cloud (XC) Mobile App Shield.

12.1.2. **"Client-Side Code"** means any code, program or other software provided by F5 to Customer, such as native libraries and SDKs, that Customer may deploy on Authorized Mobile Applications to collect or generate Shield Data.

12.1.3. **"Shield Data"** means information relating to the status of a mobile application, the device the mobile application is executed on, and the state or activities occurring on such mobile application or device, such as whether the application or device has been compromised or whether the following scenarios have been detected: mobile malware, rooting/jailbreak, debugger, code injection, app repackaging, framework injection, fake screen readers, malicious keyboards, white-box crypto, overlay attacks, man-in-the-app, or man-in-the-middle.

**Disclaimer.**

THE MOBILE APP SHIELD SDK MAY TO CAUSE ANY AUTHORIZED MOBILE APPLICATION(S) TO EXIT IF THE MOBILE APP SHIELD SDK DETERMINES THAT THE AUTHORIZED MOBILE APPLICATION(S) OR THE UNDERLYING DEVICE(S) EXECUTING THE AUTHORIZED MOBILE APPLICATION(S) ARE COMPROMISED. FOR EXAMPLE, THE MOBILE APP SHIELD SDK MAY TERMINATE AN AUTHORIZED MOBILE APPLICATION IF THE MOBILE APP SHIELD SDK DETECTS A JAVA DEBUGGER, EMULATOR, OR NATIVE HOOKS. PLEASE SEE THE DOCUMENTATION FOR MORE INFORMATION. WE HEREBY DISCLAIM ALL LIABILITY, EXPRESS OR IMPLIED, IN CONNECTION WITH THE MOBILE APP SHIELD EXITING ANY AUTHORIZED MOBILE APPLICATION(S), INCLUDING, BUT NOT LIMITED TO MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE (INCLUDING, WITHOUT LIMITATION, LOSS OF ANY INFORMATION OR STATE AND DOWNSTREAM EFFECTS, SUCH AS COMPLETING A TRANSACTION BY AN AUTHORIZED MOBILE APPLICATION OR DEPENDENT F5 SERVICES).

**Operational Terms (Stand-Alone offering):**

12.1.4. **Grant of Right.** Subject to the terms and conditions of the Agreement, any applicable Orders, and the Service Policies, we grant you a limited, non-exclusive, non-transferable, non-sublicensable license during the Service Term to:

12.1.4.1. install and execute the Client-Side Code solely on the Authorized Mobile Application(s), for the sole purpose of collecting and generating Shield Data; and

12.1.4.2. internally use the Shield Data solely to protect the Authorized Mobile Applications from tampering and reverse-engineering and solely for Customers' internal business purposes.

12.1.5. **Disclaimer.** F5 has no access to Customer Data or Shield Data in connection with the Stand-Alone offering. As such, notwithstanding anything to the contrary in the Agreement, F5 disclaims all responsibilities, obligations, and liability in connection with Customer Data (including any personal data). Shield Data is provided "as is" without warranty of any kind, and we disclaim all warranties, indemnities, and all other liabilities in connection with Shield Data.

**Operational Terms (Add-On offering):**

12.1.6. **Grant of Right.** Subject to the terms and conditions of the Agreement, any applicable Orders, and the Service Policies, we grant you a limited, non-exclusive, non-transferable, non-sublicensable license during the Service Term to:

12.1.6.1. install and execute the Client-Side Code solely on the Authorized Mobile Application(s), for the sole purpose of collecting and generating Shield Data and transmitting the Shield Data to the applicable F5 Services.

12.1.7. **DPA.** The DPA applies to personal data (as defined under the General Data Protection Regulation (Regulation (EU)2016/679) ("GDPR") that we process in providing the Distributed Cloud Mobile App Shield product.

12.1.8. **Data Protection Terms.** For details regarding the processing for the Distributed Cloud Mobile App Shield product please refer to the DPA and Schedule A below. For a description of the technical and organizational security measures for the Distributed Cloud Mobile App Shield product, please refer to Schedule B below.

**Schedule A – Distributed Cloud (XC) Mobile App Shield (Add-On offering)**

**DETAILS OF THE DATA PROCESSING**

*Details relevant to Annex I(B) of the 2021 Standard Contractual Clauses*

Applied safeguards and restrictions specific to any special categories of data: Not applicable.

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

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: Personal data is retained during the subscription term. The data will be removed after termination, subject to a reasonable period of retention of copies made for backup and business continuity purposes.

Subject matter, nature and purpose of processing, and details of processing operations: Provision of the Distributed Cloud (XC) Mobile App Shield (Add-On Offering), as described herein.

Term/Duration of Processing: As set forth in the Agreement.

Categories of Data Subjects: Individuals who interact with your mobile properties.

*Categories of Data: Internet Protocol (IP) addresses and Shield Data.

**Schedule B – Distributed Cloud (XC) Mobile App Shield (Add-On offering)**

**TECHNICAL AND ORGANISATION SECURITY MEASURES**

*Annex II of the 2021 Standard Contractual Clauses*

We will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of your Personal Data, as described in the controls included in the following:

Service Organization Control 2 Report designed to meet the applicable criteria for the security, availability and confidentiality principles set forth in TSP Section 100A, Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy by the American Institute of Certified Public Accountants.

An Attestation of Compliance Report demonstrating compliance with applicable requirements of the Payment Card Industry – Data Security Standard version 4.0.

We may replace or modify the measures described above so long as the overall security of the SaaS Offerings is not materially lowered during a subscription term.

Subprocessors will maintain commercially reasonable security through measures that may differ from those set forth above.

**13. Data Residency and Processing Reference**

https://docs.cloud.f5.com/docs/reference/data-residency-locations