F5 END USER SERVICES AGREEMENT
SERVICE-SPECIFIC TERMS

Last Updated: January 6, 2022

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.

1. Silverline SaaS Offerings

1.1 <u>Silverline Operational Terms.</u>

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

2.1 <u>Silverline DDoS Protection Service Operational Terms</u>.

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 95th 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

3.1 <u>Silverline Shape Defense Operational Terms.</u>

3.1.1 **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.

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 **Service Tier Descriptions**.

3.1.3.1 **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.

3.1.4 **Threat Data.** Notwithstanding anything to the contrary set forth herein, we will have the right to collect and analyze "Threat Data", which includes without limitation indications of compromise, telemetry and behavioral 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 related services, systems and technologies. Threat Data does not include information that identifies a natural person. 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 is our Confidential Information.

3.1.5 **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).

4. Silverline Web Application Firewall Service

4.1 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:

(a) 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).

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

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

(d) Reporting on web application firewall violation data.

(e) 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

5.1 **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 Silverline SaaS Offerings as detailed below.

5.2 **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 Appendix 1 of the 2010 Standard Contractual Clauses and 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 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

Appendix 2 of the 2010 Standard Contractual Clauses and 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. F5 Cloud Services

6.1 F5 Cloud Services Operational Terms.

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

"**Cloud Provider**" means a third-party cloud or similar environment provider which we have authorized to sell such F5 Cloud Services.

"**F5 Cloud Services**" means the cloud-based on-demand services provided by us. F5 Cloud Services are considered "SaaS Offerings" under the Agreement.

"**Non-Production Services**" means any of the F5 Cloud Services (or a component thereof) designated by us as "non-production," "test", "trial", "non-commercial," "lab," or "development".

"**Policies**" means any additional policies applicable to any F5 Cloud Service.

6.1.2 **Ordering**. You may either order F5 Cloud Services directly from us, from an Authorized Distribution Partner, or through a Cloud Provider. If you purchase F5 Cloud Services through a Cloud Provider or Authorized Distribution Partner, your use of the F5 Cloud Services will be governed by the Agreement and these Service-Specific Terms, but all terms relating to ordering, payment, taxes, and fees will be set forth in your agreement with such Cloud Provider or Authorized Distribution Partner. If you purchase F5 Cloud Services through an Authorized Distribution Partner, your order with such Authorized Distribution Partner will also set forth the description, quantity and Service Term of the SaaS Offerings that you are subscribing to through the Authorized Distribution Partner, and any pricing terms for specific SaaS Offerings as presented in the F5 Cloud Services Portal will be inapplicable.

6.1.3 **Excessive Use**. In the event of Excessive Use of an F5 Cloud Services, you agree to negotiate in good faith with your Authorized Distribution Partner to amend the applicable Order or enter into a new Order, as applicable, to increase the capacity of your subscription to cover such Excessive Use. You will place additional orders with your Partner for the SaaS Offerings each quarter during the Service Term as set forth in the amended or new Order, as applicable. In the event that you and your Partner are not able to reconcile your Excessive Use, we reserve the right to limit your usage to the capacity set forth on the applicable Order for the duration your Service Term. We may, in our sole discretion, waive Excessive Use under certain circumstances, on a case-by-case basis. No waiver of Excessive Use will entitle you to a future waiver of Excessive Use. The specific method for determining Excessive Use is provided in the description of each F5 Cloud Service.

6.1.4 **Termination - No Fixed Service Term**. If you do not have a fixed Service Term, you or F5 may terminate your Account or the Agreement at any time upon written notice to the other or at such other time as specified in the written notice. Upon such termination, you shall immediately cease using the F5 Cloud Services and the license granted to you to use such F5 Cloud Services shall automatically and immediately terminate.

6.1.5 **Non-Production Use Services**. You shall only use the Non-Production Services to conduct internal testing and development in your non-production environment. Your use of Non-Production Services may be subject to additional terms and conditions set forth in the F5 Cloud Services documentation. Unless specified in such documentation applicable to such Non-Production Services, you shall not use Non-Production Use Services in a way that involves Personal Data in the Customer Data or in a way that would pose risk to you if the relevant Non-Production Services failed in any respect. Your DPA does not apply to such Non-Production Services.

7. F5 Cloud Services – DNS Cloud Service

7.1 F5 Cloud Services – DNS Cloud Service Operational Terms

7.1.1 **Excessive Use.** For purposes of determining Excessive Use of F5 DNS Load Balancer Cloud Service, the following measurement methodologies will be used:

7.1.1.1 Number of Active Zones - If at any given point in time in the life of the contract the total zones exceeds the number indicated on your Order, it will be considered Excessive Usage.

7.1.1.2 Query Volume - If at any given 30-day period during the life of the contract the query volume exceeds the monthly contracted amount it will be considered Excessive Usage. F5 reserves the right to allow customers to burst usage beyond the monthly limits without additional penalty in its sole discretion.

8. F5 Cloud Services – DNS Load Balancer

8.1 F5 Cloud Services – DNS Load Balancer Operational Terms.

8.1.1 **Excessive Use.** For purposes of determining Excessive Use of F5 DNS Load Balancer Cloud Service, the following measurement methodologies will be used:

8.1.1.1 Number of Active Configurations / Load Balanced Records (LBRs) - If at any given point during the Service Term your total active Load Balanced Records exceeds the total contracted amount set forth on your Order, it will be considered Excessive Use.

8.1.1.2 Query Volume - If at any given 30-day period during the Service Term your query volume exceeds the monthly contracted amount set forth on your Order it will be considered Excessive Use.

8.1.1.3 Health Checks - If at any given point during the Service Term your total number per type of health checks exceeds the total contracted amount set forth on your Order, it will be considered Excessive Use.

9. F5 Cloud Services – Beacon

9.1 F5 Cloud Services – Beacon Operational Terms.

9.1.1 **Excessive Use**. For purposes of determining Excessive Use of F5 Beacon Cloud Service, the following measurement methodologies will be used:

9.1.1.1 Number of pricing units (Application/Custom Insight) – if your usage of Beacon during the Service Term exceeds the amount set forth on your Order, it will be considered Excessive Use. Use is calculated monthly and is based on the high-water mark of the number of Pricing Units reached during the preceding month.

10. F5 Cloud Services Data Protection Terms

10.1 **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 F5 Cloud Services as detailed below.

10.2 **Processing Details and Security**. For details regarding the processing for the F5 Cloud Services please refer to the DPA and Schedule A below. For a description of the technical and organizational security measures for the F5 Cloud Services, please refer to Schedule B below.

Schedule A to the F5 Cloud Services Data Protection Terms

DETAILS OF THE DATA PROCESSING

Details relevant to Appendix 1 of the 2010 Standard Contractual Clauses and Annex I(B) of the 2021 Standard Contractual Clauses

	Beacon	**DNS**	**DNS Load Balancer**
Subject Matter, Nature and Purpose of Processing and Details of Processing Operations:	Providing visibility and actionable insights into the health and performance of your applications as described above	Secondary authoritative DNS service as described above	DNS / load balancing as described above
Categories of Personal Data:	DNS / load balancing as described above monitoring and/or telemetry from devices, hosts, applications and/or services that constitutes personal data.	IP addresses and other packet header information.	IP addresses and other packet header information.
Special Categories of Data (if any):	Not applicable	Not applicable.	Not applicable
Categories of Data Subjects:	The exporter's personnel and other parties to network traffic that the exporter chooses to administer with the SaaS Offering. Depending on the exporter's usage, this could include, for example, personnel in categories such as exporter's customers, service providers, business partners, affiliates and users of exporter's website or online service.	The exporter's personnel and other parties to network traffic that the exporter chooses to administer with the SaaS Offering. Depending on the exporter's usage, this could include, for example, personnel in categories such as exporter's customers, service providers, business partners, affiliates and users of exporter's website or online service.	The exporter's personnel and other parties to network traffic that the exporter chooses to administer with the SaaS Offering. Depending on the exporter's usage, this could include, for example, personnel in categories such as exporter's customers, service providers, business partners, affiliates and users of exporter's website or online service.
Term/Duration of Processing	As set forth in the Agreement	As set forth in the Agreement	As set forth in the Agreement

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

Applied safeguards and restrictions specific to any special categories of data: No special categories of data are processed

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: As set forth in the Agreement.

Schedule B to the F5 Cloud Services Data Protection Terms

TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

Appendix 2 of the 2010 Standard Contractual Clauses and 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 level of security of the F5 Cloud Services 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.

11. Shape Security Services

11.1 Shape Security Services Operational Terms.

11.1.1 **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 components of the Shape Security Software to which you subscribe under an Order.

"**Shape Security Software**" means, collectively: (i) the proprietary software solution identified in an Order; and (ii) any Updates thereto made available by us. For the avoidance of doubt, the Shape Security Software does not include any other (or new) platforms, modules or other software not identified in an Order and that we have developed or may develop from time to time and licenses separately or license to users of the Shape Security Software for an additional fee. The Shape Security Software is a SaaS Offering under the Agreement.

11.1.2 **Grant of Right.** We grant to you a limited, revocable, non-exclusive, non-transferable, non-sublicensable right to use the Shape Security Software, subject to the terms and conditions of the Agreement, any restrictions contained in the applicable Acceptable Use Policy, and these Service-Specific Terms.

11.1.3 **Customer Responsibility.** You acknowledge and agree that you remain responsible for the security of the data being analyzed by the Shape Security Software. If using the Application Traffic Insight ("ATI") functionality of the Shape Security Software, you acknowledge and agree that a ATI identifier is not guaranteed to be unique, and F5 disclaims all liability under this Agreement in connection with your use of the ATI functionality.

11.1.4 **Threat Data**.

11.1.4.1 Notwithstanding anything to the contrary set forth herein, we will have the right to collect and analyze "Threat Data", which includes without limitation indications of compromise, telemetry and behavioral 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 Shape Security Software and related services, systems and technologies. Threat Data does not include information that identifies a natural person. 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 is our Confidential Information.

11.1.5 **Demonstration License**. With respect to Shape Security Software comprised of the ATI functionality, 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.

11.1.6 **New Data.** Certain Shape-related services 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 a 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.

11.1.7 **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 Shape Security Software in accordance with the Service Level Agreement. The terms of this Section 11.1.7 apply solely where your access to the Shape Security Software will be remote (i.e., hosted by us on our own servers or by our third party hosting services providers) and not where you have installed the Shape Security Software on physical servers or virtual machines owned or operated by you, or where your access is via Appliances delivered by us to you.

11.1.8 **Appliances**. If your access to the Shape Security Software will be via 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 this Agreement will exclusively govern and control the ordering of Appliances from us and the use of the Shape Security 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.

Shape Security Services via Volterra. Any Volterra Offerings to which Customer has access in connection with Customer's use of Shape Security Services via Volterra's cloud platform (i.e., VoltConsole) will be subject to the terms set forth in Section 17 that are applicable to such Volterra Offerings.

12. Shape Security Services Data Protection Terms

12.1 **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 Shape Security Services as detailed below.

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

Schedule A - Shape Security Services

DETAILS OF THE DATA PROCESSING

Details relevant to Appendix 1 of the 2010 Standard Contractual Clauses and Annex I(B) of the 2021 Standard Contractual Clauses

Shape Enterprise Defence (SED)

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.

Shape Application Traffic Insight (ATI)

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), ATI 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.

Shape Authentication Intelligence (Recognize)

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.

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), ATI 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.

Shape Account Protection (SAFE)

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.

Client-Side Defense (CSD)

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

Categories of Data Subjects: Not applicable.

Categories of Data: Not applicable. The CSD service does not process personal data.

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

* This asterisk above indicates that 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.

Additional details for all Shape Security Services relevant to Annex 1(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.

Schedule B to the Shape Security Services Data Protection Terms

TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

Appendix 2 of the 2010 Standard Contractual Clauses and 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 3.2.

We may replace or modify the measures described above so long as the overall security of the Shape Security Services 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. Shape Blackfish Services

13.1 Shape Blackfish Services Operational Terms.

13.1.1 Additional Definitions.

"**Attack Credential Knowledgebase**" means a data store of Evidence of Compromise collected by us as part of the Collective Defense.

"**Blackfish Solution**" means our proprietary Blackfish credential protection software and service solution. For purposes of the Agreement, the Blackfish Solution is a SaaS Offering.

"**Collective Defense**" means the participation by you (along with our other customers) to contribute Evidence of Compromise collected by us on your properties to the Attack Credential Knowledgebase and participate in the network defense.

"**Customer Account Information**" means any of the following information identified and/or collected by us or on our behalf in connection with the performance of Threat Research: (i) your compromised property (including but not limited to credentials of your customers and website/mobile application visitors); and (ii) details about accounts of your customers (including but not limited to credentials).

"**Evidence of Compromise**" means mathematical representations of user credentials determined by us to be used in an account takeover attacks on your web and mobile properties, or other evidence relevant to such account takeover attacks.

"**Threat Research**" means: (i) the collection and analysis of credentials collected while performing managed security services for you (or our other customers), including Evidence of Compromise; and (ii) security research performed by us or on our behalf using public and/or confidential sources to better understand criminal enterprises, the automated attack tools they use, the spilled credentials used in attacks on our customers' websites and mobile applications (including you), and the tactics, techniques and procedures they follow when planning and executing cyberattacks, including the collection of publicly leaked credentials.

13.1.2 **Threat Research.** Notwithstanding anything to the contrary set forth in the Agreement, or any other agreement between the parties, you acknowledge that Threat Research may result in the identification and/or collection by us of Customer Account Information and Evidence of Compromise and agree that we may use Customer Account Information and Evidence of Compromise for the benefit of you and our other customers in connection with the Blackfish Solution, or related services and product offerings.

14. Shape Blackfish Services Data Protection Terms.

14.1 **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 Shape Blackfish Services as detailed below.

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

Schedule A - Shape Blackfish Services

DETAILS OF THE DATA PROCESSING

Details relevant to Appendix 1 of the 2010 Standard Contractual Clauses and Annex I(B) of the 2021 Standard Contractual Clauses

Subject matter, nature and purpose of processing, and details of processing operations: Informing you when you send a hash of a username/credential pair to the Blackfish Services that matches one that was stolen from an unrelated third-party property.

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

Categories of Data Subjects: Data subjects whose credential information is sent to us by you to perform a check against our corpus of breached credentials.

Categories of Data: Pseudonymized usernames and credentials

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

Additional details relevant to Annex 1(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: None of the hashes that you send to Blackfish are persistently stored. The hashes are only held temporarily in volatile memory for purposes of checking against our corpus of breached credentials.

Schedule B - Shape Blackfish Services

TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

Appendix 2 of the 2010 Standard Contractual Clauses and 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 our 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.

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

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

15. Integrated Bot Defense (IBD)

15.1 **Integrated Bot Defense Operational Terms**.

15.1.1 Additional Definitions**.**

"Integrated Bot Defense Service" means the automated threat protection service delivered through an API.

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

"Excessive Use" means your usage of the Integrated Bot Defense Service in excess of the applicable Usage Metrics, as measured by us.

"Transaction" means any request from the Customer submitted to the API provided as part of the Integrated Bot Defense Service.

"SOC" means the F5 security operations center.

15.2 **Excessive Use**. We may monitor your use of the Integrated Bot Defense Service for Excessive Use. If your usage of the Integrated Bot Defense Service 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

15.3 **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 Integrated Bot Defense Service in accordance with the Service Level Agreement for SHAPE Security Software (excluding any Root Cause Analysis).

15.4 **Service Tier Descriptions**.

15.4.1 **Integrated Bot Defense Services** includes:

15.4.1.1 SOC support by phone, chat and email to maintain security policies in support of your Covered Applications, including onboarding and configuration of the Integrated Bot Defense Service.

15.5 **Threat Data.** Notwithstanding anything to the contrary set forth herein, we will have the right to collect and analyze "Threat Data", which includes without limitation indications of compromise, telemetry and behavioral 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 Integrated Bot Defense Service and related services, systems and technologies. Threat Data does not include information that identifies a natural person. 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 is our Confidential Information.

15.6 **Integrated Bot Defense via Volterra**. Any Volterra Offerings to which Customer has access in connection with Customer's use of Integrated Bot Defense via Volterra's cloud platform (i.e., VoltConsole) will be subject to the terms set forth in Section 17 that are applicable to such Volterra Offerings.

16. Integrated Bot Defense Data Protection Terms.

16.1.1 **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.

16.1.3 **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 Integrated Bot Defense Services, please refer to Schedule B below.

Schedule A - Integrated Bot Defense Services

DETAILS OF THE DATA PROCESSING

Details relevant to Appendix 1 of the 2010 Standard Contractual Clauses and Annex I(B) of the 2021 Standard Contractual Clauses

Subject Matter, Nature and Purpose of Processing, and details of processing operations: Provision of the Integrated Bot Defense Service, as described herein.

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

Categories of Data Subjects: Visitors to your Internet-facing websites protected by the Integrated Bot Defense Service

Categories of Data: Internet Protocol (IP) addresses; Integrated Bot Defense 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.

Additional details relevant to Annex 1(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.

Schedule B - Integrated Bot Defence Services

TECHNICAL AND ORGANISATION SECURITY MEASURES

Appendix 2 of the 2010 Standard Contractual Clauses and 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 3.2.

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

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

17. Professional Services

17.1 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.

17.2 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.

17.3 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.

18. Volterra Offerings

18.1 Volterra Offerings Operational Terms

18.1.1 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 Volterra Hardware from Volterra under this Agreement, such Volterra Hardware shall be deemed an "Authorized Machine" as used in this Agreement.

"**Desktop Software**" means the Volterra 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 Volterra 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 the Volterra 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.

"**Volterra Hardware**" means the server hardware component of the Volterra Offerings licensed by you as part of, or purchased by you hereunder for use in connection with, Volterra Offerings, as set forth in your Order and as further described in the Service Policies.

"**Volterra Offerings**" means Volterra SaaS Offerings, Volterra Hardware, Volterra Software, and the Volterra SDKs.

"**Volterra SaaS Offerings**" means, collectively, VoltStack™, VoltMesh™, VoltShare, and any other SaaS Offerings provided to you by us through Volterra under this Agreement, as set forth in your Order and as further described in the Service Policies.

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

"**Volterra Service Level Agreement**" means the service level agreement available at https://www.volterra.io/docs/support/sla (or any successor or related locations designated by us), as it may be updated by us from time to time

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

18.2 Access Rights.

18.2.1 Volterra SaaS Offerings. Subject to the terms and conditions of the Agreement, any applicable Orders, and the Service Policies, if your Order includes Volterra SaaS Offerings, we grant you a limited, revocable, non-exclusive, non-transferable, non-sublicensable right to (a) permit Users to access and use the Volterra 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.

18.2.2 Volterra 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 Volterra 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 Volterra 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.

18.2.3 Volterra 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:

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

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

18.3 Third-Party Access to VoltMesh. As part of the Volterra 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.

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

18.5 Purchase Price for Volterra Hardware. The purchase price for the Volterra 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 Volterra Hardware is exclusive of, and you shall be responsible for, all fees and costs for delivery, packaging, packing, shipping, carriage, and/or insurance.

18.6 Terms Applicable to Volterra Hardware.

18.6.1 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 Volterra Hardware. Volterra will use commercially reasonable efforts to ship the Volterra Hardware on or before the quoted shipment date to you or our carrier agent at Volterra's facility or the facility of our contract manufacturer, at which time risk of loss and, if you have purchased the Volterra Hardware hereunder, title, will pass to you. In the absence of specific shipping instructions from you, Volterra 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, Volterra 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 Volterra to complete deliver of the Volterra Hardware. The Volterra Hardware will be deemed accepted upon delivery to you.

18.6.2 Ownership. You agree that the Volterra Hardware shall remain the personal property of Volterra and you shall have no right, title, or interest therein. You shall keep the Volterra Hardware free from all liens,

attachments, encumbrances or judicial processes and shall not act, or fail to act, in any manner inconsistent with Volterra's 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 Volterra Hardware without Volterra's prior written consent. Notwithstanding the foregoing, if you have purchased the Volterra Hardware from Volterra hereunder, you shall retain title to such Volterra Hardware, subject to Volterra's intellectual property rights in and to the Volterra SaaS Offerings, including, without limitation, any Volterra Software embedded or installed on the Volterra Hardware.

18.6.3 Limited Hardware Warranty for Volterra Hardware. If you have purchased Volterra Hardware under this Agreement, we warrant that the Volterra Hardware will, for a period of three (3) years from the date of delivery of the Volterra 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 Volterra Hardware, or (b) issue you a credit or refund in the amount of the purchase price for such Volterra 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 Volterra Hardware to us; (iii) the defective Volterra Hardware is returned to the location specified by us; (iv) the defective Volterra 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 Volterra 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 Volterra Hardware provided to you will not extend the original warranty. The foregoing limited warranty extends only to the original Customer who purchases the Volterra 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 Volterra 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.

18.6.4 Warranty Returns. To request a return materials authorization (RMA) under the warranty provided above, please file a support ticket on VoltConsole 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.

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

18.6.6 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.

18.7 Effect of Termination. Upon termination of the Agreement, and without limiting your rights and obligations therein, if you have licensed the Volterra Hardware as part of the F5 Services, you shall promptly return to Volterra, in good

working order (reasonable and normal wear and tear excepted), at Volterra's cost using Volterra's designated shipping account, all units of Volterra Hardware. You must use the Volterra shipping containers to return the Volterra Hardware units. If you have purchased the Volterra Hardware hereunder, upon any termination or expiration of this Agreement, you shall immediately remove the Volterra Software (including any updates) from the Volterra Hardware, and destroy any copies thereof in your possession or control.

18.8 Volterra Offerings 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 Volterra Offerings as detailed below.

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

Schedule A to the Volterra Offerings Data Protection Terms

DETAILS OF THE DATA PROCESSING

Details relevant to Appendix 1 of the 2010 Standard Contractual Clauses and Annex I(B) of the 2021 Standard Contractual Clauses

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

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

Categories of Data: Data relating to individuals provided to Volterra via the Volterra 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, IP address, user identifiers, passwords, API logs, cookies, account identifier (i.e., usernames, hashed usernames), and technical data about the user's browser.

Categories of Data Subjects: Data subjects include the individuals about whom data is provided to Volterra via the Volterra 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 Volterra via the Volterra Offerings, the extent of which is determined and controlled solely by you or your end users.

Additional details relevant to Annex 1(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

Schedule B to the Volterra Offerings Data Protection Terms

TECHNICAL AND ORGANISATION SECURITY MEASURES

Volterra provides the Volterra Offerings with the same Technical and Organizational Security Measures as provided for the F5 Cloud Services outlined herein.

We may replace or modify the measures described above so long as the overall security of the Volterra 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.

19. Subprocessors; F5 Affiliates

SERVICE-SPECIFIC SUBPROCESSORS

Entity Name	Purpose	Applicable SaaS Offerings	Entity Country
Amazon Web Services, Inc.	Repository for file sharing and storing encrypted backups and cloud services hosting platform.	Silverline, Beacon, DNS, DNS Load Balancer, Essential App Protect, Shape Enterprise Defense, Volterra Offerings	United States
ZenDesk, Inc.	customer support ticket tracking.	Silverline, Beacon, DNS, DNS Load Balancer, Essential App Protect, Volterra Offerings	United States
Google LLC	Communicates monitoring alerts to customers and a messaging application.	Silverline, Volterra Offerings	United States
C-Serv Global Ltd	professional services.	Beacon, DNS, DNS Load Balancer, Essential App Protect	United Kingdom
Okta	Identity as a service and access authentication.	Blackfish, Shape Enterprise Defense	United States
Google Cloud	Hosting and storage.	Blackfish, Shape Enterprise Defense, Shape DeviceID+, Shape Recognize, Shape SAFE	United States
Stripe, Inc	Payment processing.	Volterra Offerings	United States
Databricks, Inc.	Job orchestration for cloud services.	Volterra Offerings	United States
Microsoft, Inc.	O365 productivity software.	Silverline, Beacon, DNS, DNS Load Balancer, Essential App Protect, Shape Enterprise Defense, Volterra Offerings	United States
GitLab, Inc.	Development operations platform for customer support.	Volterra Offerings	United States
Zapier, Inc.	Workflow automation for customer support.	Volterra Offerings	United States
Kentik Technologies, Inc.	DDoS monitoring and logging	Silverline DDoS Protection Service, Volterra Offerings	United States

F5 Affiliates: Subprocessors for the SaaS Offerings also include F5 Affiliates:

Entity Name	Country
F5 Networks De Argentina S.R.L.	Argentina
F5 Networks Australia Pty. Limited	Australia
F5 Networks Belgium BVBA	Belgium
FCinco Representacoes do Brasil LTDA	Brazil
F5 Networks Canada LTD.	Canada
F5 Networks Chile Limitada	Chile
F5 Networks China	China
F5 Networks Colombia S.A.S.	Colombia
F5 Networks Zagreb LLC	Croatia
F5 Networks Finland Oy	Finland
F5 Networks SARL	France
F5 Networks GmbH	Germany
F5 Networks Hong Kong Limited	Hong Kong
F5 Networks India Private Limited	India
F5 Networks Innovation Private Limited	India
F5 Networks, (Israel) Ltd.	Israel
F5 Networks SRL	Italy
F5 Networks Japan GK	Japan
F5 Networks Korea Co., Ltd.	South Korea
F5 Networks Malaysia Sdn. Bhd.	Malaysia
F5 Networks Mexico S de RL de CV	Mexico
F5 Networks Benelux B.V.	Netherlands
F5 Networks New Zealand Limited	New Zealand
F5 Networks Poland sp. z o.o.	Poland
F5 Networks Singapore Pte Ltd	Singapore
F5 Networks South Africa	South Africa
F5 Networks Iberia SL	Spain
F5 Networks Sweden Aktiebolag	Sweden
F5 Networks Taiwan Company Limited	Taiwan
F5 Networks Turkey Teknoloji Limited Sirketi	Turkey
F5 Networks Ltd	United Kingdom
F5, Inc.	United States
NGINX International Ltd	Ireland
NGINX Ltd	Russia
NGINX Asia Pacific Pte.	Singapore
Shape Security, Inc.	United States
Volterra, Inc.	United States
Volterra India Private Limited	India
Volterra SG PTE. LTD	Singapore
Acorus Networks SAS	France