

**F5 END USER SERVICES AGREEMENT  
SERVICE-SPECIFIC TERMS**

**Last Updated: June 11, 2020**

The Service-Specific Terms below govern your use of the SaaS Offerings. Capitalized terms used in these Service-Specific Terms but not defined below are defined in the End User Services Agreement or other agreement with us governing your use of the SaaS Offerings (the “**Agreement**”).

1.	Silverline SaaS Offerings .....	1
1.1	Silverline Operational Terms.....	1
2.	Silverline DDoS Protection Service .....	2
2.1	Silverline DDoS Protection Service Operational Terms.....	2
3.	Silverline Shape Defense Service.....	3
3.1	Silverline Shape Defense Operational Terms.....	3
4.	Silverline Web Application Firewall Service .....	4
4.1	Silverline Web Application Firewall Operational Terms. ....	4
5.	Silverline Data Protection Terms.....	5
5.1	Applicable DPA.....	5
5.2	Description of Processing.....	5
6.	F5 Cloud Services.....	9
6.1	F5 Cloud Services Operational Terms. ....	9
7.	F5 Cloud Services – DNS Cloud Service .....	10
7.1	F5 Cloud Services – DNS Cloud Service Operational Terms .....	10
8.	F5 Cloud Services - DNS Load Balancer .....	10
8.1	F5 Cloud Services - DNS Load Balancer Operational Terms. ....	10
9.	F5 Cloud Services - Beacon.....	10
9.1	F5 Cloud Services - Beacon Operational Terms. ....	10
10.	F5 Cloud Services Data Protection Terms. ....	11
10.1	Applicable DPA.....	11
10.2	Description of Processing:.....	11
11.	Shape Security Services .....	15
11.1	Shape Security Services Operational Terms.....	15
12.	Shape Blackfish Services.....	16
12.1	Shape Blackfish Services Operational Terms. ....	16
13.	Shape Security Services Data Protection Terms.....	16
14.	Subprocessors; F5 Affiliates. ....	16

## 1. Silverline SaaS Offerings

### 1.1 Silverline Operational Terms.

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

**“95<sup>th</sup> 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 95<sup>th</sup> 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 Service-Specific 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 Content alone or in combination with other data, such as risk score, intelligence about a threat from some source other than Customer Content, or substantiation of either of the foregoing (collectively, “New Data”). New Data does not include Customer Content. 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 agreements available at <https://www.f5.com/pdf/customer-support/eusa-sla.pdf> (“Service Level Agreement”) (or any successor or related locations designated by us), as it may be updated by us from time to time.

## **2. Silverline DDoS Protection Service**

### **2.1 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<sup>th</sup> 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 95<sup>th</sup> 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 Silverline Shape Defense Operational Terms.

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 95<sup>th</sup> 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, 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 (including, without limitation, information concerning Your data and data derived therefrom), and we will be free (during and after the Term of any Services Schedule or termination of the Agreement) to: (i) use such information and data to improve and enhance the SaaS Offerings and related services and for other development, diagnostic and corrective purposes in connection with the Shape Security Software, related services and other F5 offerings; and (ii) disclose such data solely in aggregate or other de-identified form in connection with its business.

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 95<sup>th</sup> 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 Service Tier Descriptions.

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 Applicable DPA.** To the extent that we process any personal data (as defined under the GDPR) on your behalf, in the provision of the Silverline SaaS Offerings the data processing addendum at <https://www.f5.com/pdf/customer-support/eusa-dpa.pdf> (“**Processor DPA**”) (as may be updated by us if required by applicable law) applies to Customer Content that is processed by the Silverline SaaS Offerings and, is hereby incorporated by reference, and the parties agree to comply with such terms.

**5.2 Description of Processing.** For details regarding the subject matter, nature and purpose of the processing for the Silverline SaaS Offerings under the Processor DPA, as well as the types of personal data processed and the categories data subjects, please refer to Annex A below. For a description of the technical and organizational security measures for the Silverline SaaS Offerings, please refer to Annex B below.

## Annex A

### DETAILS OF THE DATA PROCESSING

Subject Matter, Nature and Purpose of Processing: F5 Silverline SaaS Offerings

Categories of Data:

- Internet Protocol (IP) addresses associated packet metadata
- Traffic data

Special Categories of Data (if any): Not applicable, unless present in the traffic data.

Categories of Data Subjects:

- Visitors to your Internet-facing websites protected by the Silverline SaaS Offerings

*Terms of Processing:* We retain your Personal Data as set forth in the Agreement

## Annex B

### TECHNICAL AND ORGANISATION SECURITY MEASURES

F5's Silverline Data Centres – 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 organisational measures to control access to premises and facilities, particularly to check authorisation; 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 organisational (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 authorisation 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 organisational 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)

## 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.

“**Preview Services**” means any of the F5 Cloud Services (or a component thereof) designated by us as “Preview,” “Beta,” or “Evaluation Services”.

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 Content or in a way that would pose risk to you if the relevant Non-Production Services failed in any respect. Your Data Privacy Addendum does not apply to such Non-Production Services.

6.1.6 **Preview Services.** You shall use such Preview Services only for its internal demonstration, test, or evaluation purposes and not in a production environment. NOTWITHSTANDING ANY TERMS TO THE CONTRARY IN THE AGREEMENT, WE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, FOR PREVIEW SERVICES AND THEY ARE PROVIDED ON AN “AS IS” BASIS. PREVIEW SERVICES HAVE A NON-PERPETUAL TIME LIMITED SUBSCRIPTION TERM AND WE MAY “TIME-OUT” AND DISABLE THE PREVIEW SERVICES OR OTHERWISE DISCONTINUE YOUR ACCESS TO AND USE OF THE PREVIEW SERVICES AT ANY TIME WITHOUT PRIOR NOTICE. You will not attempt to defeat or circumvent any duration mechanism for Preview Services and will not use any Preview Services beyond the prescribed Service Term. Your use of Preview Services may be subject to additional terms and conditions set forth in the applicable documentation. Unless specified in such Service Policies applicable to such Preview Services, you shall not use Preview Services in a way that involves Personal Data in the Customer Content or in a way that would pose risk to you if the relevant Preview Services failed in any respect, and the Data Privacy Addendum does not apply to such Preview 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 Service Schedule, 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 Applicable DPA.** To the extent we process any personal data (as defined under the General Data Protection Regulations) on your behalf, in the provision of the Cloud Services, the Processor DPA is hereby incorporated by reference, and the parties agree to comply with such terms.

**10.2 Description of Processing:** For details regarding the subject matter, nature and purpose of the processing for the F5 Cloud Services, as well as the types of personal data processed and the categories data subjects, please refer to Annex A below.

For a description of the technical and organizational security measures for the F5 Cloud Services, please refer to Annex B below.

**Annex A**

**DETAILS OF THE DATA PROCESSING**

	<b>Beacon</b>	<b>DNS</b>	<b>DNS Load Balancer</b>
<b>Subject Matter, Nature and Purpose of Processing:</b>	F5 Cloud Services	F5 Cloud Services	F5 Cloud Services
<b>Categories of Data:</b>	Monitoring and/or telemetry from devices, hosts, applications and/or services that may constitute personal data.	IP addresses and other packet header information.	IP addresses and other packet header information.
<b>Special Categories of Data (if any):</b>	Not applicable	Not applicable.	Not applicable
<b>Categories of Data Subjects:</b>	The exporter's personnel and other parties to network traffic that the exporter chooses to administer with the Service 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 Service 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 Service 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.
<b>Term of Processing</b>	As set forth in the Agreement	As set forth in the Agreement	As set forth in the Agreement

**Annex B**

**TECHNICAL AND ORGANISATION SECURITY MEASURES**

**Security Measures.**

*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 centres 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 / tunneling: 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)

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

We may replace or modify the measures described above so long as the overall level of security for the personal data is not materially lowered.

## 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:

“**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.

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, 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 (including, without limitation, information concerning Customer Content and data derived therefrom), and we will be free (during and after the Term of any Order or termination of the Agreement) to: (i) use such information and data to improve and enhance the SaaS Offerings and related services and for other development, diagnostic and corrective purposes in connection with the Shape Security Software, related services and other F5 offerings; and (ii) disclose such data solely in aggregate or other de-identified form in connection with its business.

11.1.5 **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 Content alone or in combination with other data, such a risk score, intelligence about a threat from some source other than Customer Content, or substantiation of either of the foregoing (collectively, “New Data”). New Data does not include Customer Content. 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.

11.1.6 **Support Services.** During the Term, we will provide support services for the Shape Security Software as specified in the applicable Order.

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.



## 12. Shape Blackfish Services

### 12.1 Shape Blackfish Services Operational Terms.

#### 12.1.1 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.

12.1.2 **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.

## 13. Shape Security Services Data Protection Terms.

13.1.1 **Applicable DPA.** To the extent that any personal data (as defined under the General Data Protection Regulations) on your behalf, in the provision of the Shape Security Services, the Processor DPA is hereby incorporated by reference, and the parties agree to comply with such terms.

13.1.2 **Description of Processing.** For details regarding the subject matter, nature and purpose of the processing for the Shape Security Services under the Processor DPA, as well as the types of personal data processed and the categories data subjects, please refer to Annex A below. For a description of the technical and organizational security measures for the Shape Security Services, please refer to Annex B below.

## 14. Subprocessors; F5 Affiliates.

14.1.1 **Subprocessors List.** For a list of service-specific subprocessors and F5 affiliates, please refer to Annex C.

## Annex A

### DETAILS OF THE DATA PROCESSING

#### Shape Security Services

##### **Subject Matter, Nature and Purpose of Processing: Shape Security Services**

*Categories of Data:* Internet Protocol (IP) addresses, Android Advertising IDs, 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, mobile software development kits (SDKs) and other technical means. This data includes the following HTTP headers, and you agree not to modify such headers to include types of Personal Data not normally found in such headers, such as a username or government-issued ID number.

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

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

*Terms of Processing:* As set forth in the Agreement.

#### Shape Blackfish Services

##### **Subject Matter, Nature and Purpose of Processing: Shape Blackfish Services**

*Categories of Data:* Pseudonymized usernames and credentials

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

*Categories of Data Subjects:* Individuals who attempt to login to, or change their credentials on, your protected web and/or mobile properties.

*Terms of Processing:* As set forth in the Agreement.

## Annex B

### TECHNICAL AND ORGANISATION SECURITY MEASURES

**Security Measures. 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.

For Shape Security Services only, also an Attestation of Compliance Report demonstrating compliance with applicable requirements of the Payment Card Industry – Data Security Standard version 3.2.

We will not materially decrease the overall security of the Shape Security Services or Shape Blackfish Services during a subscription term.

**Annex C**

**SERVICE-SPECIFIC SUBPROCESSORS**

<b>Entity Name</b>	<b>Purpose</b>	<b>Applicable Services</b>	<b>Entity Country</b>
Amazon Web Services, Inc.	Repository for file sharing and storing encrypted backups. Providing cloud services hosting platform	Silverline, Beacon, DNS, DNS Load Balancer, Essential App Protect, Shape Enterprise Defense	United States
ZenDesk, Inc.	Providing Customer Support Ticket Tracking	Silverline, Beacon, DNS, DNS Load Balancer, Essential App Protect	United States
Rollbar, Inc.	Rollbar is used to store stack trace and other debugging and service improvement information about the customer portal application.	Silverline, Beacon, DNS, DNS Load Balancer, Essential App Protect	United States
New Relic, Inc.	New Relic is used to measure and monitor the performance of the customer portal application.	Silverline	United States
Google Mail	Google Mail is used to communicate monitoring alerts to customers.	Silverline	United States
Plivo Inc. Headquartered in United States	SMS-as-a-Service for customer notifications.	Silverline	United States
C-Serv Global Ltd	Providing Professional Services	Beacon, DNS, DNS Load Balancer, Essential App Protect	United Kingdom

K-Force Professional Staffing	Providing call intake for Customer Maintenance and Support	Beacon, DNS, DNS Load Balancer. Essential App Protect	United States
Skytap, Inc.	Providing virtual labs for training	Beacon, DNS, DNS Load Balancer, Essential App Protect	United States
Banc of America Merchant Services LLC	Providing credit card processing	DNS Load Balancer, Essential App Protect	United States
Avalara, Inc.	Providing tax calculation for credit card transactions	DNS Load Balancer, Essential App Protect	United States
Zuora, Inc	Providing subscription services for credit card customers	DNS Load Balancer, Essential App Protect	United States
Skytap, Inc.	Providing virtual labs for training	Beacon, DNS, DNS Load Balancer, Essential App Protect	United States
Okta	Identity as a service and access authentication	Blackfish, Shape Enterprise Defense	United States
Google Cloud	Hosting and Storage	Blackfish, Shape Enterprise Defense	United States
Equinix	Physical appliance hosting	Shape Enterprise Defense	United States

## F5 Affiliates

<b>Entity Name</b>	<b>Country</b>
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 Networks Inc.	United States