F5 Privacy Policy for Customer Support Data

Effective date: February 9, 2015; Last Updated: March 8, 2016

F5 Networks, Inc. ("F5") is committed to protecting the privacy and security of the personal data it receives from Customers. F5 has adopted this Safe Harbor Privacy Policy (the "Policy"), which sets forth how F5 may collect, use, transfer and otherwise process the Support Data (defined below) it receives from Customers in the European Economic Area and Switzerland.

This Policy complies with the Safe Harbor Principles as agreed upon by the U.S. Department of Commerce with the European Commission, as well as those agreed upon with the Swiss Federal Data Protection and Information Commissioner (collectively, the "Safe Harbor Principles"), which can be found at www.export.gov/safeharbor.

PLEASE NOTE: On October 6, 2015, the European Court of Justice issued a judgment declaring as "invalid" the European Commission's Decision 2000/520/EC of 26 July 2000 "on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce." In response to this decision, the Department of Commerce announced that it will continue to administer the Safe Harbor program, including processing submissions for self-certification to the Safe Harbor Framework. We intend to maintain our Safe Harbor Certification; *please be advised, however, that due to the ECJ's decision, Customers may no longer rely on F5's Safe Harbor certification as a basis for the transfer of personal data to the United States. EU and Swiss Customers impacted by this recent decision who are seeking an alternate compliance basis for EU-U.S. personal data transfers should contact us email at* safeharbor@f5.com.

All F5 employees who handle Customer Support Data from the European Economic Area and Switzerland are required to comply with the Principles stated in this Policy.

Capitalized terms, not otherwise defined, are defined in Section 10 of the Policy.

1. Scope of Policy

F5 provides various technology, professional and consulting services to businesses, including maintenance and support services for products. F5 may receive and process data from its Customers in order to provide its maintenance and support services, and this data may contain Personal Data. This Policy applies only to the processing of Personal Data that F5 receives in the United States from its Customers located in the European Union and Switzerland, in order to provide its maintenance and support services related to its BIG-IP, BIG-IQ and signaling delivery controller products (the "**Support Data**"). F5 is a data processor for Support Data and will only process such data on behalf of and under the instructions of its Customers.

Capitalized terms in this Policy are defined at the end of this Policy.

2. Collection and Use of Personal Data

F5 processes Support Data only for legitimate business purposes, including:

- to provide our services to Customers, to provide technical support or customer service, to respond to Customer inquiries, to send customer satisfaction surveys, or to otherwise communicate with Customers, and for accounting and billing purposes;
- to assess and improve the quality of our products, services and business operations;
- to satisfy governmental reporting and tax requirements;
- to satisfy security, health, and safety concerns;
- to plan and implement potential acquisitions and mergers;
- as required by law; and
- for other purposes consented to by Data Subjects.

We may also de-identify and/or aggregate certain data we collect such that the data can no longer reasonably be linked to a particular Customer or Data Subject. We may use this de-identified and aggregate data to improve our product and services, and for other research or statistical purposes.

We do not use Support Data for direct marketing purposes, though we may send customer satisfaction surveys to F5 Customers. F5 Customers may opt out of receiving these surveys by following the opt out instructions in the survey invitation. We may still email our Customers service and transaction related communications, even if they have opted out of receiving customer satisfaction surveys.

3. Disclosures of Personal Data

We generally disclose Support Data under the following circumstances:

- Agents and Service Providers. We may disclose Personal Data to third parties who act as agents or service providers to perform tasks on behalf of and under the instructions of F5. These third parties must agree to use such Personal Data only for the purposes for which they have been engaged by F5 and they must either: (1) comply with a mechanism permitted by the relevant European data protection authorities for transfers and processing of Personal Data (such as by signing the EU Standard Contractual Clauses); or (2) agree to provide adequate protections for the Personal Data that are no less protective than those set out in this Policy.

- Affiliates. Because F5 is a global company, Personal Data may be shared with other F5 Affiliates around the world, who act as processors or sub-processors of Support Data. The use of any Personal Data by our Affiliates will be subject to this Policy.

- Consent. F5 may also disclose Personal Data for other purposes or to other third parties, when a Data Subject has consented to such disclosure.

- Additional Disclosures**.** We may also disclose Personal Data and Sensitive Data (i) where required by law; (ii) where necessary to protect the health and safety of others; (iii) where necessary for the establishment of legal claims or defenses, to obtain legal advice, or as evidence in litigation; (iv) to defend our rights and property; (v) in the event of a

reorganization, sale or transfer of our assets; and (vi) where such data manifestly made public by the Data Subject.

Sensitive Data. F5 does not intentionally collect Sensitive Data from Customers. We do not request Sensitive Data from Customers. If we receive any Customer's Support Data that contains Sensitive Data, we will treat it in accordance with this Policy and will only process such data on behalf of and under the instructions of that Customer.

4. Data Integrity and Security

F5 uses reasonable efforts to maintain the accuracy and integrity of Personal Data. F5 also uses reasonable physical, administrative and technical safeguards designed to protect against the loss, misuse and alteration of data that we collect or maintain. For example, all electronically stored Personal Data is stored on a secure network with monitored firewall protection, and access to F5's electronic information systems requires user authentication via password or similar means. Despite these precautions, no data security safeguards guarantee 100% security all of the time.

5. Right to Access, Change or Delete Personal Data

Customers are responsible for responding to access requests from Data Subjects (e.g., the Customers' employees or end users) related to the Support Data that F5 receives and processes for Customer. To the extent a Customer requests information about the Personal Data it has provided to F5 as Support Data, F5 will take reasonable steps to accommodate such request where necessary to permit customer to respond to an access request.

6. Changes to this Policy

This Policy may be amended from time to time, consistent with the Safe Harbor Principles and applicable data protection and privacy laws and principles. If we make changes to the Policy that materially affect the way we handle the Personal Data we have already collected from you, we will attempt to notify you and allow you to opt-out of having your Personal Data used in any materially different manner.

7. Questions or Complaints

Customers may contact F5 with questions or complaints concerning this Policy at safeharbor@f5.com.

8. Enforcement and Dispute Resolution

As part of our annual Safe Harbor re-certification process, F5 will periodically review this Policy for accuracy, as well as for conformity with the Safe Harbor Principles and applicable data privacy and protection laws.

If you have any questions, complaints or disputes regarding the manner in which F5 handles or protects your Personal Data, please contact us at safeharbor@f5.com. F5 will promptly

investigate and attempt to resolve complaints and disputes in a manner that complies with the principles described in this Policy.

For any complaints related to this Policy that cannot be resolved through our internal process, we agree to participate in the dispute resolution procedures set forth by JAMS. More information about the JAMS International Safe Harbor Program is available here. If we or the appointed arbitrator(s) conclude that we did not comply with this Policy, we will take appropriate steps to address any adverse effects and assure our future compliance.

9. Defined Terms

The defined terms in this Policy have the following meanings:

"**Data Subject**" means an identified or identifiable natural living person. An identifiable person is one who can be identified, directly or indirectly, by reference to a name, or to one or more factors unique to his or her personal physical, psychological, mental, economic, cultural or social characteristics.

"**Customer**" means a current or former partner, vendor, supplier, customer, or client of F5, who is also a resident of the European Economic Area or Switzerland. The term shall also include any agent, employee, or representative of a Customer whose Personal Data F5 has obtained as part of its business relationship with the Customer.

"**Affiliate**" means an affiliated or subsidiary company of F5 Networks, Inc.

"**Personal Data**" means any information that identifies or could be used to identify a particular Data Subject, including but not limited to name, contact information, identification number, title, and any information that is associated with such identifiable data. Personal Data does not include data that is publicly available, or is anonymous or de-identified, including any other data through which individuals are no longer identifiable, or identifiable only with a disproportionately large expense in time, cost or labor.

"**Sensitive Data**" means Personal Data that discloses a Data Subject's medical or health condition; race or ethnicity; political, religious or philosophical affiliations or opinions; sexual orientation; criminal background; or trade union membership.