SUPPORT AND PROFESSIONAL SERVICES

DATA PROTECTION ADDENDUM

This Data Protection Addendum ("**DPA**") forms part of each Agreement between Customer and F5 for F5's provision to Customer of the Support Services or Professional Services.

1. Definitions

1.1 "**Agreement**" means the direct agreement between F5 and you pursuant to which F5 provides the Services, which is the F5 Maintenance Terms and Conditions (for Support Services), the F5 Consulting Services Agreement (for Professional Services), or a negotiated alternative for the same services. The term does not include any contract with a reseller, distributor, or similar intermediary of F5's services.

1.2 "**Applicable Law**" means all laws, regulations and other legal requirements applicable to either (i) F5 in its role as provider of the Services or (ii) you. This may include, for example, the General Data Protection Regulation (Regulation (EU) 2016/679) ("**GDPR**"), equivalent requirements in the United Kingdom including the UK General Data Protection Regulation and the Data Protection Act 2018 ("**UK Data Protection Law**"), and the California Consumer Privacy Act and associated regulations ("**CCPA**"). Each party is responsible only for the Applicable Law applicable to it.

1.3 "**Controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

1.4 "**Customer**" means the entity to which F5 provides the Services pursuant to such Agreement.

1.5 "**Personal Data**" means any information relating to an identified or identifiable individual, within the meaning of the GDPR (regardless of whether the GDPR applies), and any other information constituting "personal information" as such term is defined in the CCPA (regardless of whether the CCPA applies).

1.6 "**Personal Data Breach**" means the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data.

1.7 "**Process**" and "**Processing**" mean any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, creating, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.8 "**Processor**" means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.

1.9 "**Services**" refers to one or both of the following, as the context requires:

1.9.1 "**Support Services**," which are the services that F5 provides to you pursuant to the F5 Maintenance Terms and Conditions or pursuant to a negotiated alternative for the same services.

1.9.2 "**Professional Services**," which are the services F5 provides to you pursuant to the F5 Consulting Services Agreement pursuant to a negotiated alternative for the same services.

1.10 "**Standard Contractual Clauses**" refers for Personal Data subject to the GDPR, the "2021 Standard Contractual Clauses," defined as the clauses issued pursuant to the EU Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, available at http://data.europa.eu/eli/dec_impl/2021/914/oj and completed as described in the "Data Transfers" section below.

1.11 "**Subprocessor**" means any F5 affiliate or subcontractor engaged by F5 for the Processing of Personal Data.

1.12 "**Support Portal**" means support.f5.com and any similar online property that F5 operates for the purpose of providing support information or receiving support inquiries for the Service.

1.13 "**UK Addendum**" means the "International Data Transfer Addendum to the EU Commission Standard Contractual Clauses" issued by the Information Commissioner under s.119A(1) of the Data Protection Act 2018

1.14 "**You**" means Customer.

1.15 "**Your Content**" refers to one or both of the following, as the context requires:

1.15.1 For Support Services: data you upload in iHealth, data you provide in a support ticket in the Support Portal, data you provide to F5 support personnel by telephone, and data present on an F5 Product that you return to F5 through the RMA process.

1.15.2 For Professional Services: data of yours that F5 professional services personnel review or otherwise process when providing Professional Services to you.

1.16 Other capitalized terms have the meaning set forth in the Agreement.

2. Scope and Relationship of the Parties

2.1 This DPA applies only to the Personal Data in Your Content.

2.2 For such Personal Data, you are (or you represent that you are acting with full authority on behalf of) the Controller, and F5 is your Processor. If you are acting on behalf of a Controller (or on behalf of intermediaries such as other Processors of the Controller), then, to the extent legally permissible:

2.2.1 You will serve as the sole point of contact for F5 with regard to any such third parties;

2.2.2 F5 need not interact directly with any such third party in matters relating to this DPA; and

2.2.3 Where F5 would otherwise be required to provide information, assistance, cooperation, or anything else to such third party, F5 may provide it solely to you; but

2.2.4 F5 is entitled to follow the instructions of such third party with respect to such third party's Personal Data instead of your instructions if F5 reasonably believes this is legally required under the circumstances.

3. Your Instructions to F5

3.1 F5 will Process the Personal Data only as described in the Agreement, unless obligated to do otherwise by Applicable Law. In such case, F5 shall inform you of that legal requirement before the Processing unless legally prohibited from doing so.

3.2 The details of the Processing are set forth in Schedule 1.

3.3 The Agreement, including this DPA, along with your configuration of any settings or options in the Service (as you may be permitted to modify from time to time, depending on the Service), constitute your complete and final instructions to F5 regarding the Processing of Personal Data, including for purposes of the Standard Contractual Clauses, if they apply.

3.4 You will comply with Applicable Law relevant to your use of the Services, including by obtaining any consents and providing any notices required under Applicable Law for F5 to provide the Services. You will ensure that you are entitled to transfer the Personal Data to F5 so that F5 and its Subprocessors may lawfully Process the Personal Data in accordance with this DPA.

3.5 You shall not instruct F5 to Process Personal Data in violation of Applicable Law. F5 shall promptly inform you if, in F5's opinion, an instruction from you infringes Applicable Law.

4. Subprocessors

4.1 F5 may subcontract the collection or other Processing of Personal Data in compliance with Applicable Law. Prior to a Subprocessor's Processing of Personal Data, F5 will impose contractual obligations on the Subprocessor that are substantially the same as those imposed on F5 under this DPA. New Subprocessors will be notified to you prior to their Processing of Personal Data by an update to the Support and Professional Services Subprocessors List posted at https://www.f5.com/company/policies (or a similarly accessible successor location that F5 specifies there or by notice to you under the Agreement), unless exigent circumstances require their earlier Processing of Personal Data, in which case the new Subprocessor will be notified to you as soon as practicable.

4.2 You may object to F5's use of a new Subprocessor by notifying F5 within ten (10) business days after receipt of an updated Subprocessor list. In the event you reasonably object to a new Subprocessor, as permitted in the preceding sentence, F5 will use reasonable efforts to make available to you a change in the Service or recommend a commercially reasonable change to your use of the Service to avoid Processing of Personal Data by the objected-to Subprocessor without unreasonably burdening you. If F5 is unable to make available such a change or recommendation within a reasonable period of time, not exceeding thirty (30) days, you may terminate the affected Service that cannot be provided by F5 without the use of the objected-to Subprocessor by providing written notice to F5. F5 will refund to you any prepaid fees covering the remainder of the term of such Service following the effective date of termination with respect to such terminated Services, without imposing a penalty for such termination on you. If you do not object to use of the new Subprocessor and terminate as set forth above, the Subprocessor is deemed to be accepted by you. F5

remains liable for its Subprocessors' performance to the same extent F5 is liable for its own performance.

5. Security

5.1 F5 will assist you in your compliance with the security obligations of the GDPR and other Applicable Law, as relevant to F5's role in Processing the Personal Data, taking into account the nature of Processing and the information available to F5, by complying with the following paragraph, by making available the Support Portal subject to its terms, and, if available in the applicable Service, by providing security options. You are solely responsible for determining whether and how to use such options within the scope of the Agreement, and F5 shall have no liability for damage arising from your failure to select and properly use the security options most appropriate to your use of the Service.

5.2 To protect the Personal Data, F5 shall implement technical and organizational measures described in the applicable Service Specific Terms, without prejudice to F5's right to make future replacements or modifications to the measures that do not materially lower the level of security of the Personal Data.

5.3 You are solely responsible for reviewing any available security documentation and features and evaluating for yourself whether the Service and related security meet your needs, including your security obligations under Applicable Law. You may use the Service only if the security commitments in this DPA would provide a level of security appropriate to the risk in respect of the Personal Data.

5.4 F5 will ensure that the individuals F5 authorizes to Process the Personal Data (i) are subject to a written confidentiality agreement covering such data or are under an appropriate statutory obligation of confidentiality and (ii) receive training appropriate to their role in the Processing of the Personal Data.

6. Personal Data Breach Notification

6.1 F5 will comply with the Personal Data Breach-related obligations directly applicable to it under the GDPR and other Applicable Law. Taking into account the nature of Processing and the information available to F5, F5 will assist you in complying with those applicable to you by informing you without undue delay after becoming aware of a confirmed Personal Data Breach of the Personal Data F5 or its Subprocessors received from or on behalf of Customer. Such notification is not an acknowledgement of fault or responsibility. To the extent available, this notification will include F5's then-current assessment of the following, which may be based on incomplete information:

6.1.1 The nature of the Personal Data Breach, including, where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of Personal Data records concerned;

6.1.2 The likely consequences of the Personal Data Breach; and

6.1.3 Measures taken or proposed to be taken by F5 to address the Personal Data Breach, including, where applicable, measures to mitigate its possible adverse effects.

7. Assistance Responding to Data Subjects

7.1 Taking into account the nature of the Processing, F5 will assist you with the fulfillment of your obligation to honor requests by individuals to exercise their rights under the GDPR and other Applicable Law (such as rights to access their Personal Data) by providing the Service's admin capabilities (where applicable) and by forwarding to you any such requests or Personal Data-related complaints that F5 receives within a commercially reasonable timeframe. This timeframe will not exceed five (5) business days if (i) the request or complaint is received through the privacy contact information

specified in the F5 privacy notice that is hyperlinked from the home page of F5.com and (ii) the request or complaint identifies you as the F5 customer to whom it pertains. Additional support for such requests may be available and would require mutual agreement on fees, the scope of F5's involvement, and any other terms that the parties deem appropriate.

8. Assistance with DPIAs and Consultation with Supervisory Authorities

8.1 Taking into account the nature of the Processing and the information available to F5, F5 will provide reasonable assistance and cooperation to you for your performance of any legally required data protection impact assessment of the Processing or proposed Processing of the Personal Data involving the relevant Services, and with related consultation with supervisory authorities, by providing you with documentation for the relevant Services, by making available the Support Portal subject to its terms, and by complying with the Audit section below. Additional support for data protection impact assessments or relations with regulators may be available and would require mutual agreement on fees, the scope of F5's involvement, and any other terms that the parties deem appropriate.

9. Data Transfers

9.1 You authorize F5 and its Subprocessors to make international transfers of the Personal Data in accordance with this DPA so long as Applicable Law for such transfers is respected.

9.2 The 2021 Standard Contractual Clauses, completed as set out below in clause 9.4 of this Agreement shall also apply to transfers of such Personal Data, subject to sub-clause 9.3 below.

9.3 Tables 1 to 3 of the UK Addendum shall be deemed completed with relevant information from the 2021 Standard Contractual Clauses, completed as set out above, and the options "neither party" shall be deemed checked in Table 4. The start date of the UK Addendum (as set out in Table 1) shall be the date of this Agreement

9.4 To the extent legally required, the Standard Contractual Clauses form part of this DPA and take precedence over the rest of this DPA to the extent of any conflict, and (except as described in Section 9.5) they will be deemed completed as follows:

9.4.1 To the extent you act as a controller and F5 acts as your processor with respect to the Personal Data subject to the Standard Contractual Clauses, its Module 2 applies. To the extent you act as a processor and F5 acts as your Subprocessor with respect to the Personal Data subject to the Standard Contractual Clauses, its Module 3 applies.

9.4.2 Clause 7 (the optional docking clause) is included.

9.4.3 Under Clause 9 (Use of sub-processors), the parties select Option 2 (General written authorization). The initial list of sub-processors is set forth in the Support and Professional Services Subprocessors list available at https://www.f5.com/company/policies, and F5 shall update that list at least 10 days in advance of any intended additions or replacements of sub-processors.

9.4.4 Under Clause 11 (Redress), the optional requirement that data subjects be permitted to lodge a complaint with an independent dispute resolution body does not apply.

9.4.5 Under Clause 17 (Governing law), the parties choose Option 1 (the law of an EU Member State that allows for third-party beneficiary rights). The parties select the law of Ireland.

9.4.6 Under Clause 18 (Choice of forum and jurisdiction), the parties select the courts of Ireland.

9.4.7 Under Annex I(A) of the Standard Contractual Clauses (List of parties):

9.4.7.1 The exporter is you.

9.4.7.2 The exporter's contact information for F5 to use is as set forth in the ordering document for the Services. The exporter's contact information for data subjects to use is set forth in its privacy policy, as are the identity and contact details of the exporter's data protection officer (if any) and representative in the European Union (if any).

9.4.7.3 The exporter's activity as relevant to the data transferred under these Clauses is its use of the relevant Service(s).

9.4.7.4 The importer is F5. The importer's mailing address is set forth in the Agreement or in the ordering document for the Services, and its email address is privacy@f5.com, subject to an update by F5 of those addresses in accordance with the Agreement.

9.4.7.5 The importer's activity as relevant to the data transferred under these Clauses is its provision of the relevant Service(s).

9.4.7.6 When you subscribe to a particular Service, the parties are deemed to be signing Annex I(A) of the Standard Contractual Clauses.

9.4.8 For any particular Service, the details for Annex I(B) of the Standard Contractual Clauses (Description of transfer) are set forth in Schedule 1 of the DPA.

9.4.9 Under Annex I(C) of the Standard Contractual Clauses (Competent supervisory authority), the parties shall follow the rules for identifying such authority under Clause 13 and, to the extent legally permissible, select the Irish Data Protection Commission.

9.4.10 Annex II of the Standard Contractual Clauses (Technical and organizational measures) is set forth in Schedule 2 of the DPA.

9.4.11 Annex III of the Standard Contractual Clauses (List of Subprocessors) is inapplicable.

9.5 For transfers of Personal Data that are subject to the Swiss Federal Act on Data Protection ("**FADP**"), the Standard Contractual Clauses form part of this DPA as set forth in Section 9.4 of this DPA, but with the following differences to the extent required by the FADP:

9.5.1 References to the GDPR in the Standard Contractual Clauses are to be understood as references to the FADP insofar as the data transfers are subject exclusively to the FADP and not to the GDPR.

9.5.2 The term "member state" in the Standard Contractual Clauses shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the Standard Contractual Clauses.

9.5.3 References to personal data in the Standard Contractual Clauses also refer to data about identifiable legal entities until the entry into force of revisions to the FADP that eliminate this broader scope.

9.5.4 Under Annex I(C) of the Standard Contractual Clauses (Competent supervisory authority):

9.5.4.1 Where the transfer is subject exclusively to the FADP and not the GDPR, the supervisory authority is the Swiss Federal Data Protection and Information Commissioner.

9.5.4.2 Where the transfer is subject to both the FADP and the GDPR, the supervisory authority is the Swiss Federal Data Protection and Information Commissioner insofar as the transfer is governed by the FADP, and the supervisory authority is as set forth in Section 9.2.9 of this DPA insofar as the transfer is governed by the GDPR.

10. Audits

10.1 F5 will make available to you all information reasonably necessary to demonstrate compliance with this DPA, and allow for and contribute to audits including inspections, conducted by you or another auditor mandated by you, as follows:

10.1.1 If the requested audit scope is addressed in an ISO or other audit report issued by a third-party auditor within the prior twelve (12) months and F5 provides such report to you and confirms that there are no known material changes in the controls audited, you agree to accept the findings presented in the report in lieu of requesting an audit of the same controls covered by the report. The report is Confidential Information of F5.

10.1.2 If not covered by such report, F5 will provide a written description of its compliance measures for this DPA. This is Confidential Information of F5. You may also refer to the applicable Service documentation and the Support Portal, subject to its terms, as applicable.

10.1.3 You agree to exercise any right you may have to conduct an audit or inspection, including under the Standard Contractual Clauses, if they apply, by instructing F5 to provide the report and/or information described above. If you wish to change this instruction regarding the audit, you may request a change to this instruction by sending F5 written notice as provided for in the Agreement. Such additional support may be available and would require mutual agreement on fees you would be charged, audit scope, the scope of F5's involvement, and any other terms that the parties deem appropriate.

10.1.4 Nothing in this DPA will require F5 to disclose or make available:

10.1.4.1 any data of any other customer of F5;

10.1.4.2 access to systems;

10.1.4.3 F5's accounting or financial information;

10.1.4.4 any trade secret of F5;

10.1.4.5 any information or access that, in F5's reasonable opinion, could (A) compromise the security of F5 systems or premises; or (B) cause F5 to breach its obligations under Applicable Law or applicable contracts; or

10.1.4.6 any information sought for any reason other than the good faith fulfillment of your obligations under Applicable Law to audit compliance under this DPA.

11. Return or Destruction

11.1 F5 will, at your choice, return to you and/or destroy all Personal Data after the termination or expiration of your subscription to the relevant Service except to the extent Applicable Law requires storage of the Personal Data. F5's return of Personal Data to you may be subject to reasonable fees for such return. If F5 has not received your election within 30 days of such termination or expiration, F5 may assume that you have selected deletion. The certification of deletion required by the Standard Contractual Clauses (if they apply) will be provided only on written request.

11.2 Nothing will oblige F5 to delete Personal Data from files created for security, backup and business continuity purposes sooner than required by F5's reasonable data retention processes. If you require earlier deletion of such Personal Data, and such deletion is commercially feasible, you must first pay F5's reasonable fees for such deletion, which may include costs for business interruptions associated with such a request.

Schedule 1: Details of The Data Processing

Subject Matter, Nature and Purpose of Processing, and details of processing operations: Provision of the Support Services and/or Professional Services pursuant to the Agreement.

Term/Duration of Processing: As set forth in the Agreement and any applicable Order.

Categories of Data Subjects: The Personal Data transferred may concern current and prospective customers, users and employees of the exporter, as determined by the exporter.

Categories of Data: This is determined by the exporter, but it may contain personally identifiable technical information (including, for example, IP addresses).

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

Applied safeguards and restrictions specific to any special categories of data: Not applicable. In any case, the same high standard of protection described in Schedule 2 to 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: As set forth in the Agreement and any applicable Order.

Schedule 2: Technical and Organisation 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, usernames, 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.

Access Levels: System access levels are based on the rule of least privilege and are defined for each user role. IT administrators configure access to the most restrictive level possible that still enables the user to effectively perform their job. Permissions that exceed the normal access levels associated with a given job assignment require additional authorization from management and in some cases, additional logging, monitoring, and auditing.

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)

Auditing access rights and privileges, on regular cadence, of authorized end-users with access to in-scope systems, applications, and information.

A vulnerability management program that addresses emerging threats and risk to in-scope systems, and applications.

Change Management program, which governs changes to IT infrastructure.

Testing and auditing controls, which address compliance with our information security requirements.

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

Specific technical and organisational measures to be taken by the importer to be able to provide assistance to the data exporter: The nature of the Services is assistance to the data exporter. For Support Services, the Agreement details how this assistance may be requested, and F5 maintains extensive technical infrastructure to provide such assistance, such as its iHealth tool for Support Services. Professional Services customers may submit requests for assistance through the channels establishes for such requests in the context of the particular engagement.