DATA PROCESSING ADDENDUM – PLATFORM ONE™

1.   Scope and Order of Precedence.

This Data Processing Addendum ("**DPA**") is an addendum to the Extreme Platform ONE Services Agreement ("Agreement") between Extreme (as defined in the Agreement) and the Customer identified in the signature blocks below and applies to Extreme's processing of Customer Personal Data in the course of providing the Cloud Service. This DPA is incorporated into, and made a part of, the Agreement. In the event and to the extent of any conflict between this DPA and the Agreement, this DPA shall control. This DPA will be effective until Extreme is no longer Processing Customer Personal Data. All capitalized terms not defined in this DPA will have the meanings set forth in the Agreement.

2.   Definitions.

In this DPA, the following capitalized bold terms will have the following meanings:

"**Cloud Service**" means any cloud service offering provided by Extreme to Customer pursuant to the Agreement.

"**Controller**," "**Processor**," "**Data Subject**," "**Personal Data**," "**Personal Data Breach**," and "**Processing**" each have the meaning set forth in the GDPR.

"**Customer**" means you, the end user customer using the Cloud Service.

"**Customer Personal Data**" means Personal Data provided to Extreme by Customer for Processing by Extreme in connection with the Cloud Service. Customer Personal Data includes Personal Data of the Customer's network users and Personal Data of third parties which Customer provides to Extreme as a result of Customer's use of the Cloud Service (including as a result of services Customer provides to such third parties).

"**Data Protection Laws**" means the applicable privacy or data protection law, which could include, but is not limited to:

- EU General Data Protection Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC;
- UK Data Protection Act 2018
- California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 *et seq.*, as amended, and its implementing regulations
- The Lei Geral de Proteção de Dados ("LGPD") of Brazil

"**GDPR**" means EU General Data Protection Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC.

"**Standard Contractual Clauses**" means the standard contractual clauses approved by the European Commission for the transfer of Personal Data to Processors established in third countries under the applicable EU Data Protection Laws, as amended, replaced, or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR.

"**Sub-processor**" means a subcontractor Extreme engages who, as part of the subcontractor's role of providing the Cloud Service, will Process Customer Personal Data.

3.   **Categories of Personal Data & Data Subjects, Duration and Purpose of the Processing.**

3.1   To perform the Cloud Service, Customer hereby instructs Extreme to Process the following categories of Customer Personal Data:

- Unique device IDs and usage and location information, such as MAC addresses, IP addresses, device names, and location-based data, collected from end user devices in conjunction with their network access by means of the Cloud Service (or services Customer may provide), along with any other Customer Personal Data provided by Customer in unstructured data; and

- Depending on Customer's configuration of services, Customer Personal Data may include end user name, email address, and/or phone number utilized for guest access.

3.2   To perform the Cloud Service, Customer hereby instructs Extreme to Process the Customer Personal Data.

3.3   This DPA will apply and be enforceable as long as Extreme provides the Cloud Service under the Agreement requiring Processing of Customer Personal Data and such Customer Personal Data has not been returned to Customer or deleted subject to Section 12.

3.4   The purpose of the Processing is to enable Extreme to provide the Cloud Service to Customer under the Agreement

4.   **Customer's Instructions.**

4.1   Customer may provide instructions from time-to-time in writing to Extreme with regard to Processing of Customer Personal Data in addition to those specified herein. Extreme shall process the Customer Personal Data only on documented instructions from the Customer (including the instruction to provide the Cloud Service under the Agreement), including with regard to transfers of Customer Personal Data to a third country or an international organisation, unless required to do so by applicable Data Protection Laws or other applicable law or regulation to which Extreme is subject; in such a case, Extreme shall inform the Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. Extreme will use commercially reasonable efforts to comply with all such instructions without additional charge to the extent necessary for Extreme to comply with its obligations to Customer as set forth in the Agreement. The parties will negotiate in good faith with respect to any other change in the Cloud Service and/or fees resulting from any additional instructions.

4.2   Customer warrants that all Customer Personal Data Processed by Extreme in accordance with Customer's instructions has been and shall be provided by Customer to Extreme in accordance with Data Protection Laws, including, without limitation: (a) ensuring that all notifications to and approvals from regulators which may be required by Data Protection Laws are made and maintained by Customer,

and (b) ensuring that all Customer Personal Data is collected and processed lawfully, is accurate, and that Customer has established a lawful basis for Processing of the Customer Personal Data to be undertaken by Extreme pursuant to the Agreement. Customer shall indemnify and hold Extreme harmless against all losses, fines and regulatory sanctions arising from any claim by a third party or regulator arising from any breach of this Section 4.2.

5.   Roles and Restrictions on Processing of Customer Personal Data.

5.1   Customer will at all times:

(a) remain the Controller of Customer Personal Data pursuant to Data Protection Laws;

(b) determine the purposes and means of its Processing of Customer Personal Data, including issuing instructions to Extreme regarding such Processing; and

(c) comply with the obligations applicable to it pursuant to Data Protection Laws regarding the Processing of Customer Personal Data, including, without limitation, establishing a legal basis for the Processing hereunder by Extreme of Customer Personal Data.

5.2   Extreme is a Processor with respect to its Processing of Customer Personal Data hereunder. Extreme will Process Customer Personal Data solely for the provision of the Cloud Service, and will not otherwise:

(a) Process Customer Personal Data for purposes other than those set forth in the Agreement or as instructed by Customer in accordance with Section 4, unless Processing is required by Data Protection Laws or other applicable laws or regulation to which Extreme is subject, in which case Extreme, shall, to the extent permitted by applicable law, inform the Customer Member of that legal requirement before the relevant Processing of that Customer Personal Data important grounds of public interest, or

(b) disclose such Customer Personal Data to third parties other than Sub- processors, as permitted or required by the Agreement, Data Protection Laws, or as instructed by Customer in accordance with this Section 4, this DPA.

5.3   Taking into account the nature of the Processing and the information available to Customer, Extreme will provide Customer with necessary assistance in Customer's compliance efforts under the Data Protection Laws in relation to undertaking data protection impact assessments and with any prior consultations to any supervisory authority.

5.4   Extreme will comply with the obligations applicable to it pursuant to Data Protection Laws regarding the Processing of Customer Personal Data, including Extreme's obligation to promptly inform Customer if, in Extreme's opinion, a processing instruction from Customer infringes on the Data Protection Laws and/or other EU data protection provisions or other Union or Member State data protection provisions.

5.5   Extreme will treat the Customer Personal Data as confidential, and will ensure that its employees or other personnel have agreed in writing (electronically or in any other manner) to protect the confidentiality and security of Customer Personal Data.

6.   Rights of Data Subjects.

6.1   Taking into account the nature of the Processing, Extreme will assist Customer upon request by technical and organizational measures, insofar as this is possible and necessary, to respond to Data Subject requests for exercising the Data Subject's rights granted under Data Protection Laws with regard to their Personal Data held in Extreme's information technology environment.

6.2   Extreme will promptly pass on to the Customer any requests of an individual Data Subject for exercising the Data Subject's rights granted under Data Protection Laws with regard to Customer Personal Data Processed by Extreme in connection with the Cloud Service or instruct the Data Subject to contact Customer directly to make such request; Extreme is not responsible for responding directly to the request, unless otherwise required by Data Protection Laws.

7.   Cross Border and Onward Data Transfers.

7.1   Transfers of Customer Personal Data originating from the EEA, UK or Switzerland to Extreme or Sub-processors located in countries outside the EEA, UK or Switzerland that have not received a binding adequacy decision by the European Commission or by a competent national data protection authority, are subject to (a) the terms of the Standard Contractual Clauses incorporated into this DPA by reference attached hereto; or (b) other appropriate transfer mechanisms pursuant to Data Protection Laws.

7.2   For the purposes of the Standard Contractual Clauses, the parties agree that (a) Customer will act as the data exporter on Customer's own behalf and on behalf of any of its entities and (b) Extreme will act on its own behalf as the data importer. This DPA shall be read in conjunction with the Standard Contractual Clauses or other appropriate transfer mechanisms.

8.   Affiliates and Sub-processors.

8.1   Some or all of Extreme's obligations under the Agreement may be performed by Subprocessors. Extreme maintains a list of Sub-processors that may Process Customer Personal Data. Extreme will provide a copy of that list to Customer upon request.

8.2   The Sub-processors will be required to abide by substantially the same obligations as Extreme under this DPA as applicable to their Processing of Customer Personal Data. Extreme remains responsible at all times for compliance with the terms of this DPA by its Sub-processors.

8.3   Customer consents to Extreme's use of Sub-processors in the performance of the Cloud Service in accordance with the terms of Sections 7 above, and this Section 8. Extreme will notify Customer of the addition or replacement of Sub-processors, which may be provided by email to the administrator or notification within ExtremeCloud Services. If Customer does not object in writing to DPA@extremenetworks.com within thirty days of receipt of the notice, then Customer is deemed to have accepted such Sub-processor. If Customer does object

in writing to DPA@extremenetworks.com within thirty days of receipt of the notice, Extreme and Customer will discuss possible resolutions.

9.   Technical and Organizational Measures.

Extreme maintains appropriate technical and organizational security measures for the Processing of Customer Personal Data, including measures specified in this Section 9 to the extent applicable to Extreme's Processing of Customer Personal Data. These measures are intended to protect Customer Personal Data against accidental or unauthorized loss, destruction, alteration, disclosure, or access, and against all other unlawful forms of Processing.

- **Encryption**. For the Cloud Service, Extreme secures all data at rest and data in transit using industry standard encryption protocols and methods and managing all cryptographic controls within the solution. When ExtremeCloud SD-WAN customers transmit log files which could contain personal data, encryption details and processes are determined jointly with the customer.

- **Physical Access Control**. Extreme employs measures designed to prevent unauthorized persons from gaining access to data processing systems in which Customer Personal Data is Processed, such as the use of security personnel, secured buildings, and data center premises.

- **System Access Control**. The following may, among other controls, be applied depending upon the particular Cloud Service licensed: authentication via passwords and two-factor authentication, documented authorization processes, documented change management processes, and logging of access on several levels. For Cloud Service hosted at Extreme: (i) log-ins to the Cloud Service environment by Extreme employees and Third Party Sub-processors are logged; (ii) logical access to the data centers is restricted and protected by firewall/VLAN; and (iii) intrusion detection systems, centralized logging and alerting, and firewalls are used.

- **Data Access Control**. Customer Personal Data is accessible and manageable only by properly authorized staff AND direct database query and application access rights are established and enforced.

- **Input Control**. Customer Personal Data source is under the control of the Customer, and Personal Data integration into the system, is managed by secured file transfer (*i.e.*, via web services) from the Customer to the extent possible or preferred by the Customer.

- **Data Backup**. For Cloud Service hosted at Extreme: back-ups are taken on a regular basis; backups are secured using a combination of technical and physical controls, depending on the particular Cloud Service.

- **Data Segregation**. Customer Personal Data from different Extreme customers' environments and/or locations is logically segregated where practicable on Extreme's systems to the extent possible.

- **Confidentiality.** Extreme employees and Sub-processors having access to Customer Personal Data are subject to confidentiality arrangements as set out in Section 5 of the Agreement.

10. Audit Rights

10.1 Customer has the right to inspect upon reasonable advance written notice and subject to appropriate confidentiality safeguards and restrictions Extreme's respective systems and facilities up to one (1) time every twelve (12) months (except in response to a Personal Data Breach or where required by a supervisory authority) to ensure compliance with this DPA only to the extent required by Data Protection Laws.

10.2 Before the commencement of any such audit, Customer and Extreme shall mutually agree in good faith upon the scope, and duration of the audit. Any inspection must be conducted
during regular business hours at the applicable facility, subject to Extreme's policies, and may not unreasonably interfere with Extreme's business activities.

10.3 Customer is entitled to conduct the audit either by an authorized representative or through an independent third-party auditor, provided that the auditing party is not a competitor to Extreme. Any authorized representatives of Customer (including third parties) must comply with the confidentiality requirements under this DPA and the Agreement; the results of such audit will be deemed the confidential information of Extreme.

10.4 Customer shall notify Extreme with information regarding any non-compliance discovered during an audit. Any audits are solely at the Customer's expense and Customer will reimburse Extreme for any reasonably incurred costs. Any request for Extreme to provide assistance with an audit is considered a separate service if such audit assistance requires the use of resources different from or in addition to those required for the provision of the Cloud Service.

10.5 Upon Customer's reasonable request, Extreme will make available to Customer all information necessary to demonstrate compliance with the obligations set out in Article 28
GDPR.

11. Incident Management and Breach Notification.

11.1 Extreme evaluates and responds to incidents that create suspicion of or indicate a Personal Data Breach. Extreme operations staff is instructed to respond to Personal Data Breach as required pursuant to Data Protection Laws.

11.2 Extreme will notify Customer without undue delay after Extreme becomes aware of a Personal Data Breach that involves Customer Personal Data.

11.3 Extreme will promptly investigate any such Personal Data Breach and take reasonable measures to identify its root cause(s) and prevent a recurrence. As information is collected or otherwise becomes available, unless prohibited by applicable law, Extreme will provide Customer with a description of the Personal Data Breach, the type of Personal Data that was the subject of the Personal Data Breach, and other information Customer may reasonably request concerning the affected Data Subjects.

11.4   The parties agree to coordinate in good faith on developing the content of any related public statements. Extreme will assist Customer, as necessary, to facilitate any required notices for the affected Data Subjects and/or notices to the relevant data protection authorities.

12.   Return and Deletion of Personal Data upon End of Cloud Service.

12.1   Subject to Section 12.2, following termination of the Cloud Service and in conjunction with Section 7 of the Agreement, Extreme will make available for retrieval to the Customer, or delete, anonymize, or otherwise render unrecoverable all Customer Personal Data then available in Extreme's information technology environment that holds Customer Personal Data.

12.2   Extreme and its Sub-processors may retain Customer Personal Data to the extent required by applicable Data Protection Law or other law or regulation to which Extreme is subject or as is otherwise described in the Agreement.

13.   Legally Required Disclosures.

Except as otherwise required by applicable law to which Extreme is subject, Extreme will promptly notify Customer of any subpoena, judicial, administrative, or arbitral order of an executive or administrative agency, regulatory agency, or other governmental authority ("**Demand**") that it receives and which relates to the Processing of Customer Personal Data. Where such a Demand is made on Customer, Extreme will, at Customer's reasonable request, provide Customer with necessary information in its possession that may be responsive to the Demand and any assistance reasonably required for Customer to respond to the Demand in a timely manner. Customer acknowledges that Extreme has no responsibility to interact directly with the entity making the Demand.

EXTREME NETWORKS, INC., on behalf of itself and its affiliates, including, but not limited to, Extreme Networks Ireland Ops Unlimited Company	**CUSTOMER** Company Name:
	By:
By:	Name:
Name: John Morrison	Title:
Title: Senior Vice President of Sales	

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

(b) The Parties:

  (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

  (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer') have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU)

---

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

2016/679 and, with respect to data transfers from controllers to processors and/or processors

to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

MODULE TWO: Transfer controller to processor

8.1   Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2   Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3   Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4   Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5   Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to

the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the

information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[2] (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii)the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

---

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9   Documentation and compliance

(a)   The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b)   The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c)   The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d)   The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e)   The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

(a)   OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least **30 days** in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[3] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to

protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

MODULE TWO: Transfer controller to processor

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

---

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

MODULE TWO: Transfer controller to processor

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

MODULE TWO: Transfer controller to processor

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its subprocessor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

MODULE TWO: Transfer controller to processor

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

MODULE TWO: Transfer controller to processor

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

  (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved, and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

  (ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant

in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[4] (12);

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal

---

[4] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

MODULE TWO: Transfer controller to processor

15.1   Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary, with the help of the data exporter) if it:

   (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal

   data requested, the requesting authority, the legal basis for the request and the response provided; or

   (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2   Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii)the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) [For Modules One, Two and Three: Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data.] The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

MODULE TWO: Transfer controller to processor

OPTION 1: These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of **Ireland**.

Clause 18

Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of **Ireland** (specify Member State).

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieve through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I A.

LIST OF PARTIES

MODULE TWO: Transfer controller to processor

Data exporter(s): [Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]

1.   Name: …

Address: …

Contact person's name, position and contact details: …

==Activities relevant to the data transferred under these Clauses: …==

==Signature and date: …==

Role (controller/processor): …**Controller**

2.   …

Data importer(s): [Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]

1.Name: … **Extreme Networks Inc.**

Address: …**2121 RDU Center Dr., Suite 300, Morrisville, NC 27560 USA**

Contact person's name, position and contact details: … **privacyinquiries@extremenetworks.com**

Activities relevant to the data transferred under these Clauses: … **Enterprise cloud networking management**

<mark style="background:cyan">Signature and date: …</mark>

Role (controller/processor): …**processor**

2.   …

B.   DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

Categories of data subjects whose personal data is transferred

… **users of data exporter's network**

Categories of personal data transferred

For Extreme AI

- **Unique device IDs and usage and location information, such as MAC and IP addresses and location-based data, collected from end user' devices in conjunction with their internet access by means of the Cloud Service (or services Customer may provide) (as**

terms are defined in the DPA), as well as unstructured data that may be entered by users; and

• **Depending on Data Exporter's configuration of services, end user name, email address, and/or phone number utilized for guest access.**

For ExtremeCloud IQ:

• **Unique device IDs and usage and location information, such as MAC and IP addresses and location-based data, collected from end user' devices in conjunction with their internet access by means of the Cloud Service (or services Customer may provide) (as terms are defined in the DPA); and**

• **Depending on Data Exporter's configuration of services, end user name, email address, and/or phone number utilized for guest access.**

For ExtremeCloud SD-WAN Solution:

• **Unique device IDs and usage and location information, such as MAC and IP addresses**

For XIQ-Business Insights

• **Unique device IDs and usage and location information, such as MAC and IP addresses, IMEI and location-based data, collected from end user' devices in conjunction with their internet access by means of the Cloud Service (or services Customer may provide) (as terms are defined in the DPA).**

For AI Studio:

• **Unique device IDs and usage and location information, such as MAC and IP addresses and location-based data, collected from end user' devices in conjunction with their internet access by means of the Cloud Service (or services Customer may provide) (as terms are defined in the DPA); and depending on Data Exporter's configuration of services, end user name, email address, and/or phone number utilized for guest access, as well as other information provided by the user in unstructured data.**

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised

training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

… **N/A**

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

… **continuous**

Nature of the processing

… **collection, recording, organization, structuring, storage, adaptation or alteration retrieval use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, and destruction**

Purpose(s) of the data transfer and further processing

… **enterprise cloud networking management and support**

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

For all Cloud Services, data existing at the RDC at the time of termination of the agreement will be retained for 30 days following termination.

… **For ExtremeCloud IQ and AI Studio:**

- **During the Term of the Agreement, data retention varies depending on the data center selected by the Data Exporter.**

For ExtremeCloud SD-WAN Solution:

- **Quantity of reporting data is reduced periodically (i.e., historical data is retained initially on an up-to-the minute basis, and older data is eventually available only on an hourly basis)**
- **Log files are rotated depending on volume of activity on the platform**

For XIQ-Business Insights

Raw data flows from within the EU are deleted within 15 days, and aggregated data is hashed and salted within 30 days.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

… **For ExtremeCloud IQ, XIQ Business Insights, and AI Studio:**

- **Data is transferred to sub-processors for data hosting**
- **Log files that may contain IP addresses, MAC addresses, or device names may be transferred to Data Importer's affiliates if technical assistance is requested by Data Exporter**

For ExtremeCloud SD-WAN Solution:

- **Log files that may contain IP addresses or MAC addresses may be transferred to Data Importer's affiliates if technical assistance is requested by Data Exporter**

C.   COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer controller to processor

Identify the competent supervisory authority/ies in accordance with Clause 13

… **[[to be completed by Data Exporter]]**

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE TWO: Transfer controller to processor

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

- **Encryption.** **For ExtremeCloud IQ, Extreme secures all data at rest and data in transit using industry standard encryption protocols and methods and managing all cryptographic controls within the solution. When ExtremeCloud SD-WAN customers transmit log files which could contain personal data, encryption details and processes are determined jointly with the customer.**

- **Physical Access Control.** **Extreme employs measures designed to prevent unauthorized persons from gaining access to data processing systems in which Customer Personal Data is Processed, such as the use of security personnel, secured buildings, and data center premises.**

- **System Access Control.** **The following may, among other controls, be applied depending upon the particular Cloud Service ordered: authentication via passwords and two-factor authentication, documented authorization processes, documented change management processes, and logging of access on several levels. For Cloud Service hosted at Extreme: (i) log-ins to the Cloud Service environment by Extreme employees and Sub-processors are logged; (ii) logical access to the data centers is restricted and protected by firewall/VLAN; and (iii) intrusion detection systems, centralized logging and alerting, and firewalls are used.**

- **Data Access Control.** **Customer Personal Data is accessible and manageable only by properly authorized staff and direct database query and application access rights are established and enforced.**

- **Input Control.** **Customer Personal Data source is under the control of the Customer, and Personal Data integration into the system is managed by secured file transfer (i.e., via web services) from the Customer to the extent possible or preferred by the Customer.**

- **Data Backup.** **For Cloud Service hosted at Extreme: back-ups are taken on a regular basis; backups are secured using a combination of technical and physical controls, depending on the particular Cloud Service.**

- **Data Segregation.** **Customer Personal Data from different Extreme customers' environments and/or locations is logically segregated where practicable on Extreme's systems to the extent possible.**

- **Confidentiality.** **Extreme employees and Sub-processors having access to Customer Personal Data are subject to confidentiality arrangements as set out in Section 5 of the Agreement.**

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

For all ExtremeCloud Services:

- Technical support may be provided by employees of these entities when Customer requests support or technical assistance. The technical and organizational measures described above apply to all of these entities.
  - Extreme Networks India Private Limited, Extreme Networks Technology (Beijing) Co. Ltd., Extreme Networks APAC Sdn. Bhd., Aerohive Networks (Hangzhou) Ltd., Extreme Networks Canada, Inc., Extreme Networks, s.r.o.

For ExtremeCloud IQ:

- **Hosting provider (based on Data Exporter's selection)** o **https://aws.amazon.com/compliance/gdpr-center/ (Amazon Web Services)** o **https://cloud.google.com/security/gdpr (Google Cloud Platform)**
  - **https://www.microsoft.com/en-us/trust-center/product-overview (Microsoft Azure)**
- **https://www.salesforce.com/company/legal/trust-and-compliancedocumentation/ (Salesforce.com)**

For ExtremeCloud SD-WAN Solution:

- **https://www.salesforce.com/company/legal/trust-and-compliancedocumentation/ (Salesforce.com)**
- **https://www.microsoft.com/en-us/trust-center/product-overview (Microsoft Azure)**

ANNEX III LIST

OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

EXPLANATORY NOTE:

This Annex must be completed for Modules Two and Three, in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).

The controller has authorised the use of the following sub-processors:

1.Name: … *[[N/A – Option 2 selected]]*

Address: …

Contact person's name, position and contact details: …

Description of processing (including a clear delimitation of responsibilities in case several subprocessors are authorised): …

…

UK Addendum to the EU Commission Standard Contractual Clauses

[[applicable only where Data Exporter is exporting personal data from the UK]]

Part 1: Tables

Table 1: Parties

	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Start date		
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: Trading name (if different): Main address (if a company registered address): Official registration number (if any) (company number or similar identifier):	Full legal name: **Extreme Networks, Inc.** Trading name (if different): **2121 RDU Center Dr., Suite 300, Morrisville, NC 27560 USA** Main address (if a company registered address): Official registration number (if any) (company number or similar identifier):
Key Contact	Full Name (optional): Job Title: Contact details including email:	Full Name (optional): Job Title: Contact details including email: **privacyinquiries@extremenetworks.com**
Signature (if required for the purposes of Section 2)		

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: see date of execution of SCCs Reference (if any): Other identifier (if any): Or the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1						
2	X	X	Optional language not included	General	30 days	
3						
4						

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: see SCCs

Annex 1B: Description of Transfer: see SCCs

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: see SCCs

Annex III: List of Sub processors (Modules 2 and 3 only): see SCCs

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ~~Importer~~ ~~Exporter~~ neither Party

Part 2: Mandatory Clauses
Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs. **Interpretation of this Addendum**

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.

Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 1 .
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into. **Hierarchy**

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

    c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

    a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

    b. In Clause 2, delete the words:

       "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

    c. Clause 6 (Description of the transfer(s)) is replaced with:

       "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

d. Clause 8.7(i) of Module 1 is replaced with:

> "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

> "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

f. References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:

> "the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

> "These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

> "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11. **Amendments to this Addendum**

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

    a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or

    b. reflects changes to UK Data Protection Laws;

    The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

    a. its direct costs of performing its obligations under the Addendum; and/or

    b. its risk under the Addendum,

    and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.