ANNEX 1 – PROCESSING OF CUSTOMER PERSONAL DATA

1. You warrant that You are the data controller in respect of the Personal Data, or that You are authorized by the data controller to issue instructions to Extreme under this Agreement in respect of such data.

2. You shall comply with Your obligations under the Data Protection Law in respect of the Personal Data (including Your provision to, or making it available for collection by, Extreme), and shall ensure that Your instructions to Extreme do not result in processing in breach of the Data Protection Law. The categories of Customer Personal Data to be processed by Extreme and the processing activities to be performed under this Annex are set out in the relevant Service Specifications.

3. Subject at all times to Your obligations under the Agreement, Extreme undertakes to:

   a) only process Customer Personal Data in accordance with Your documented instructions, unless required to do otherwise by applicable law. In which event, Extreme shall inform You of the legal requirement before processing Customer Personal Data other than in accordance with Your instructions, unless that same law prohibits Extreme from doing so on important grounds of public interest;
   b) implement appropriate technical and organizational measures to protect any Customer Personal Data processed by it against unauthorized and unlawful processing and against accidental loss, destruction, disclosure, damage or alteration;
   c) ensure those of Extreme's personnel who are involved in processing the Customer Personal Data are bound by appropriate obligations of confidentiality;
   d) inform the Customer promptly, and in any event within seven (7) days, if Extreme receives (i) a request from a data subject to have access to his/her Customer Personal Data; or (ii) a complaint or request relating to Your obligations under the Data Protection Law;
   e) taking into account the nature of the processing and the information available to You, provide You with reasonable assistance in ensuring compliance with Your obligations under the Data Protection Law in relation to security, data breach notification, data protection impact assessments, prior consultation, audits and inspections, where applicable from time to time;
   f) make available to You (or Your third party appointees bound by appropriate obligations of confidentiality) such records as You may reasonably require to demonstrate compliance by Extreme with Your obligations; and
   g) within fourteen (14) days following termination of the Agreement, Extreme shall, at Your direction: (i) return all Customer Personal Data to You; or (ii) destroy all such Customer Personal Data unless prohibited from doing so by any applicable law.

4. Subject to any provisions of the Agreement to the contrary, Extreme shall not appoint any third party to process the Customer Personal Data ("**Subprocessor**") other than: (a) with Your prior consent; and (b) by way of a written agreement with the Subprocessor which imposes equivalent obligations in relation to the security of the processing on the Subprocessor as are imposed on Extreme under this Annex. You warrant that You generally consent to Extreme appointing a Subprocessor, provided that Extreme informs You of any intended changes concerning the addition or replacement of other Subprocessors, and gives You an opportunity to object to such changes on reasonable grounds.

5. You hereby consent to the Customer Personal Data being processed anywhere in the world throughout the duration of this Agreement, subject to Extreme's continued compliance with this Section 5. However, to the extent that any Customer Personal Data to which the Data Protection Law of the European Economic Area (EEA) applies is processed outside the EEA, the terms of the transfer shall be governed by the EU Standard Contractual Clauses for the transfer of Customer Personal Data to processors attached as the Schedule to this Agreement, which are hereby incorporated into this Agreement and which shall prevail to the extent of any conflict with this Agreement.

Schedule: Standard Contractual Clauses

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation: ……
Address: ……
Tel. ……fax ……..; e-mail: ……..
Other information needed to identify the organisation
……
……
……
(the data **exporter**)

And

Name of the data importing organisation: ……
Address: ……
Tel. ……; fax ……; e-mail: ……
Other information needed to identify the organisation:
……
……
……
(the data **importer**)

each a 'party'; together 'the parties',

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions
For the purposes of the Clauses:

(a)'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [(1)];
(b) 'the data exporter' means the controller who transfers the personal data;
(c)'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
(d)'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
(e)'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
(f)'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer
The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause
1.The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2.The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3.The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.
4.The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer [(2)]

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

  (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

  (ii) any accidental or unauthorised access; and

  (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;
(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6
Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.
   The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.
3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7
Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8
Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9
Governing law

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely …

Clause 10
Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11
Sub-processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses [3]. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.
2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party

liability of the sub-processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely …
4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data-processing services

1. The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

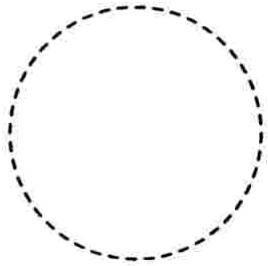
On behalf of the data exporter:

Name (written out in full): ……..

Position: ……

Address: ……

Other information necessary in order for the contract to be binding (if any):

	Signature …

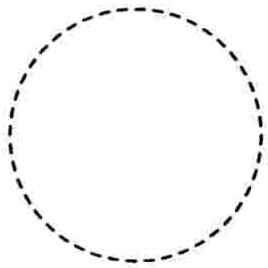
On behalf of the data importer:

Name (written out in full): ……..

Position: ……

Address: ……

Other information necessary in order for the contract to be binding (if any):

	Signature …

(1) Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

(2) Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

(3) This requirement may be satisfied by the sub-processor co-signing the contract entered into between the data exporter and the data importer under this Decision.

Appendix 1
to the Standard Contractual Clauses

Data exporter
The data exporter is the end customer for whom the data importer is providing the relevant services (whether the end customer acquires the services through a partner or directly from Extreme).

Data importer
The data importer is Extreme Networks, Inc.

Data subjects
The personal data transferred concern the following categories of data subjects:

For ExtremeCloud, see http://bit.ly/2s7zadf
For ExtremeLocation, see http://bit.ly/2x51wLd
For ExtremeWorks, see http://bit.ly/2s7Hn1h
For Managed Services, see http://bit.ly/2IGaUWL

Categories of data
The personal data transferred concern the following categories of data:

For ExtremeCloud, see http://bit.ly/2s7zadf
For ExtremeLocation, see http://bit.ly/2x51wLd
For ExtremeWorks, see http://bit.ly/2s7Hn1h
For Managed Services, see http://bit.ly/2IGaUWL

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data (please specify):

N/A

Processing operations
The personal data transferred will be subject to the following basic processing activities (please specify):

For ExtremeCloud, see http://bit.ly/2s7zadf
For ExtremeLocation, see http://bit.ly/2x51wLd
For ExtremeWorks, see http://bit.ly/2s7Hn1h
For Managed Services, see http://bit.ly/2IGaUWL

Appendix 2
to the Standard Contractual Clauses

General Controls & Governance
Extreme Networks takes a comprehensive approach to Information Security, including data protection and SDLC. The tone is set from the top with an executive sponsored InfoSec Steering Committee whose responsibilities include policy oversight, incident response review, strategy alignment, and performance management. The governing body has representation from all key business functions.

Access
All access is controlled by a centrally-integrated UAM ecosystem driven by HR. All access is based on a "least privileged" basis down to the role level within applicable applications.

Any access to a system, part of a system, or data is strictly controlled on a "needs only" basis in association with the person's role and responsibilities within the organization. All access control principles are detailed in our Information Security Policies and guidelines. These policies cover prohibited acts, such as copying, reading and access of any data that is not directly connected to the person's role.

All access to systems, as stated previously, is controlled per role. Shared accounts are strictly prohibited. Application logging is used as applicable.

Personnel
Extreme endeavors to ensure that only the best talent is part of the Extreme family. As part of this mandate, we take reasonable steps to ensure that no person is appointed to a position unless that person:
a) Is competent and qualified to perform the specific tasks assigned to them;
b) Has been instructed in the requirements relevant to the performance of the obligations of their role, including the handling of personal data; and
c) Has signed a non-disclosure or other confidentiality agreement that applies to not just to Extreme confidential information, but also to confidential information of Extreme's customers and other third parties that we receive in confidence.

Physical Security
All media destruction is governed by Extreme's digital disposal policy. This complements the data retention policy on when and for how long data should be retained within the organization. All core systems within the enterprise are covered by back-up solutions allowing for retrieval of accidentally deleted data.

All locations are badge controlled with access only granted on a needs basis.

Incident Management
Extreme takes seriously any security incident that could impact Extreme assets, whether physical or virtual. In line with regulatory and contractual requirements, we focus in particular on data security and rapid assessment of whether any security incident could impact or has impacted confidential data, including personal data.

All InfoSec team members undergo regular training on the latest tools and technologies.

Data Protection
Extreme policy mandates that all corporate data, including that of our customers and partners, must only be stored on corporate systems that are fully backed up and protected. All network and system events are tracked and monitored as part of our centralized InfoSecOp's management program. Full logging is in place as applicable to facilitate monitoring and investigations.

The environment is protected from common threats using industry standard approaches including, but not limited to:

- Web application firewalls
- Intrusion detection and prevention systems
- Infrastructure vulnerability scanning
- Penetration testing
- Web application vulnerability scanning