EXTREME NETWORKS

DATA PROTECTION AND SECURITY ADDENDUM

This Data Protection and Security Addendum ("**Addendum**") is made between Extreme Networks, Inc., with a primary office at 2121 RDU Center Drive, Suite #300, Morrisville, NC 27560, and its affiliates ("**Extreme**") and Vendor and its affiliates identified in the Services Agreement and/or on the face of the purchase order ("**Vendor**"). Extreme and Vendor are collectively referred to as the "Parties" herein.

This Addendum is governed by the terms of the applicable agreement entered into by the Parties for Vendor's services (the "**Services Agreement**"). In the event of a conflict between this Addendum and the Services Agreement, including the exhibits hereto, this Addendum shall control, but only with respect to the subject matter contained herein.

In consideration of the mutual promises and covenants contained herein and of other good and valuable consideration, the receipt of which is hereby acknowledged, the Parties agree as follows:

1. **PARTS OF AGREEMENT.**

1.1 This Addendum consists of these general terms and the following exhibits:

Exhibit 1: Definitions

Exhibit 2: Security Requirements,

Exhibit 3: Controller-Process Terms, including:

Schedule 1: Description of Personal Data Processing; and

Schedule 2: Standard Contractual Clauses, including: Annexes 1 and 2 to the Standard Contractual Clauses

2. **PURPOSE.**

2.1 This Addendum describes Vendor's obligations regarding processing of Personal Data and the minimum information security requirements that Vendor must meet and maintain to protect Personal Data from unauthorized use, access, disclosure, theft, manipulation, reproduction, or Security Breach or otherwise during the term of any Services Agreement and for any period thereafter during which Vendor or any third party has possession of, or access to, any Personal Data. Vendor's ongoing adherence to the terms of this Addendum is an express condition to Vendor's doing business with Extreme.

2.2 Extreme may request a change to this Addendum from time to time, upon reasonable prior notice to Vendor, provided that no changes shall be applicable to Vendor until Vendor and Extreme agree to the changes and execute an amendment to this Addendum.

3. **GENERAL PROVISIONS.**

3.1 Vendor's failure to comply with any of the provisions of this Addendum is a material breach of this Addendum. In such event, Extreme may terminate this Addendum, the

Services Agreement, and/or any Statement of Work then in effect, immediately upon written notice to Vendor, without further liability or obligation by Extreme.

3.2 This Addendum shall be co-terminus with the Services Agreement.

3.3 Notwithstanding any limitation of liability provision in the Services Agreement to the contrary, Vendor shall defend, indemnify and hold harmless Extreme and its affiliates, and their respective officers, directors, employees, agents, successors and permitted assigns (each an "**Indemnitee**") from and against all losses, damages, liabilities, deficiencies, actions, judgments interest, awards, penalties, fines costs or expenses of whatever kind, including reasonable attorney's fees, the cost of enforcing any right to indemnification hereunder the cost of pursuing any insurance providers, arising out of or resulting from any third-party claim against any Extreme Indemnitee arising out of or resulting from Vendor's failure to comply with any of its obligations under this Addendum.

-Exhibit 1 follows this page-

EXHIBIT 1

DEFINITIONS

The following terms, as used in this Addendum (including all Exhibits), have the meanings ascribed to them, as provided below.

"**Authorized Persons**" means Vendor's employees and contractors who have a need to know or otherwise access Personal Data to enable Vendor to perform its obligations under this Addendum.

"Confidential Information" means any data or information, including, but not limited to, Personal Data, business plans, proprietary software, product development plans, bidding and pricing procedures, market plans and strategies, sales forecasts and projections, internal performance statistics, financial data, pricing, blueprints, designs, specifications, customer and employee information, technical information, internal information regarding security practices, risk assessments, protocols, security testing and other measures and technology used in support of network security, computer programs, manufacturing and customer lists, business and contractual relationships and terms and conditions of contracts disclosed to Vendor by Extreme in any manner, whether orally, visually or in tangible form and all copies thereof, whether created by Extreme or Vendor.

"Data Protection Law" shall mean all applicable laws, regulations, directives and standards relating to data protection and privacy, which may include (without limitation) the EU Data Protection Directive (95/46/EC) as implemented in each jurisdiction, the EU General Data Protection Regulation (2016/679) ("GDPR"), the EU Privacy and Electronic Communications Directive 2002/58/EC as implemented in each jurisdiction, and any amending or replacement legislation from time to time; the California Consumer Privacy Act of 2018, Cal. Civ. Code Sec. 1798.100 et seq., as amended; the Brazilian General Data Protection Law, Federal Law no. 13,709/2018, and any amending legislation from time to time.

"**Extreme Information**" means information or data provided to, accessed by, and/or processed by Vendor on Extreme's behalf. Extreme Information may include Confidential Information, which includes Personal Data.

"**Personal Data**" means data that is provided to Vendor, to which access was provided to Vendor, or is processed by Vendor, by or at the direction of Extreme, in the course of Vendor's provisioning of services under a Services Agreement that is identified by applicable Data Protection Law as personal data. Personal Data typically includes data that directly or indirectly identifies, relates to, or links to an identifiable natural person, such as: names, addresses, telephone numbers, e-mail addresses, browsing history, purchase history, photographs, recordings, IP addresses and other unique identifiers. Personal Data also includes categories of sensitive personal data, as defined by applicable Data Protection Law, which may include information relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health status, biometrics, genetics, sexual orientation, government-issued identifiers, financial account identifiers, and precise geolocation. Personal Data is deemed to be Confidential Information of Extreme.;

"**Security Breach**" means (i) any act or omission that compromises the security, data or integrity of Extreme Information or the physical, technical, administrative or organizational safeguards put in place by Vendor that relate to the protection of the security, confidentiality or integrity of Extreme Information, or (ii) receipt of a complaint in relation to the privacy practices of Vendor or a breach or alleged breach of this Addendum relating to such privacy practices.

-Exhibit 2 follows this page-

EXHIBIT 2

1. **SECURITY POLICY**

1.1 Vendor acknowledges and agrees that, in the course of its engagement by Extreme, Vendor may receive or have access to Extreme Information. Vendor shall comply with the terms and conditions set forth in the Addendum (including this Exhibit 2), in its collection, receipt, transmission, storage, disposal, use and disclosure of such Extreme Information and be responsible for the unauthorized collection, receipt, transmission, access, storage, dispose, use and disclosure of Extreme Information under its control or in its possession by all Authorized Persons. Vendor shall be responsible for, and remain liable to, Extreme for the actions or omissions of all Authorized Persons concerning the treatment of Extreme Information.

1.2 This Addendum does not limit other obligations of Vendor, including under the Services Agreement or laws that apply to Vendor or Vendor's performance under the Services Agreement under the Data Protection Laws or otherwise with regard to the Extreme Information.

1.3 Extreme Information is deemed to be Confidential Information of Extreme and not of the Vendor.

1.4 In recognition of the foregoing, Vendor acknowledges and agrees that, in the course of its providing Services to Extreme, Vendor may receive or have access to Extreme Information, and thereby agrees that it shall:

(a) maintain all Extreme Information in strict confidence, using reasonable care to avoid unauthorized access, use or disclosure;

(b) use and disclose Extreme Information solely and exclusively for the purposes for which Extreme Information, or access to it, is provided pursuant to the terms and conditions of this Addendum and the Services Agreement, and not to use, sell, rent, loan, lease, transfer, distribute, or otherwise disclose or make available Extreme Information for Vendor's own purposes or for the benefit of anyone other than Extreme, in each case, without Extreme's prior written consent; and

(c) not directly or indirectly, disclose Extreme Information to any person other than its Authorized Personnel, including any subcontractors, agents or outsourcers without Extreme's express written consent, unless and to the extent required by government authorities or to the extent expressly required by applicable law. In any case, Vendor shall be responsible for, and remain liable to Extreme for the actions and omissions of such unauthorized parties concerning the treatment of such Extreme Information as if they were Vendor's own actions and omissions.

2. INFORMATION SECURITY.

2.1 Vendor represents and warrants that its collection, access, use, storage, disposal and disclosure of Personal Data does and will comply with all applicable Data Protection Laws, as well as all other applicable laws or regulations.

2.2 Without limiting Vendor's obligations under Section 2.1 above, Vendor will implement and maintain physical, administrative and technical safeguards and other security measures to protect Extreme Information that are no less rigorous than accepted industry practices for information security, and shall ensure that all such safeguards, including the manner in which Extreme Information is collected, accessed, used, stored, processed, disposed of and disclosed, comply with applicable Data Protection Laws, as well as the terms and conditions of this Addendum.

2.3 If, in the course of its engagement by Extreme, Vendor has access to or will collect, access, use, store, process, dispose of or disclose credit, debit or other payment cardholder information, Vendor shall at all times remain in compliance with the Payment Card Industry Data Security Standard ("**PCI DSS**") requirements, including remaining aware at all times of changes to the PCI DSS and promptly implementing all procedures and practices as may be necessary to remain in compliance with the PCI DSS, in each case, at Vendor's sole cost and expense.

2.4 As a minimum, Vendor's safeguards for the protection of Extreme Information shall include:

2.4.1 limiting access to Extreme Information to Authorized Persons;

2.4.2 securing business facilities, data centers, paper files, servers, back-up systems and computing equipment, including, but not limited to all mobile devices another equipment with information storage capability;

2.4.3 implementing network, device applicable, database and platform security;

2.4.4 security information transmission, storage and disposal;

2.4.5 implementing authentication and access controls within media, application, operating systems and equipment;

2.4.6 encrypting Extreme Information stored on any mobile media;

2.4.7 encrypting Extreme Information transmitted over public or wireless networks;

2.4.8 implementing appropriate personal security and integrity procedures and practices, including, but not limited to, conducting background checks consistent with applicable law; and

2.4.9 providing appropriate privacy and information security training to Vendor's employees and contractors.

2.5 Vendor shall also comply with the following requirements during the longer of the term of the Services Agreement and the duration of time that Vendor holds Extreme Information:

2.5.1 Vendor will install and maintain a working network firewall to protect data accessible via the Internet and will keep all Extreme Information protected by the firewall at all times.

2.5.2 Vendor will keep its systems and software up-to-date with the latest upgrades, updates, bug fixes, new versions and other modifications necessary to ensure security of the Extreme Information.

2.5.3 Vendor will at all times use anti-malware software and will keep the anti-malware software up to date at system installation locations. Vendor will mitigate threats from all viruses, spyware, and other malicious code that are or should reasonably have been detected by up-to-date anti-malware software.

2.5.4 Vendor will regularly test its security systems and processes to ensure they meet the requirements of this Addendum Policy.

2.5.5 Operating systems must be patched at least quarterly during the system lifecycle. Operating systems must be on a currently supported platform and must never run-on deprecated versions which are not currently under support.

2.5.6 Insecure protocols such as Telnet, FTP and HTTP, which allow credentials to pass in clear text, must never be used.

2.6 Vendor will secure Extreme Information, including by complying with the following requirements:

2.6.1 Vendor will assign a unique ID to each person with computer access to Extreme Information.

2.6.2 Vendor will regularly review the list of people and services with access to Extreme Information and remove accounts that no longer require access. This review must be performed at least once every ninety (90) days during the system lifecycle.

2.6.3 Vendor will not use manufacturer-supplied defaults for system passwords and other security parameters on any operating systems, software or other systems. Vendor will mandate and ensure the use of system-enforced "strong passwords" in accordance with the best practices (described below) on all systems hosting, storing, processing, or that have or control access to, Extreme Information and will require that all passwords and access credentials are kept confidential and not shared among personnel. All Vendor's systems hosting, storing, processing, or that have or control access to Extreme Information must be compatible with single sign-on (SSO) implementation.

2.6.4 Password best practices. Passwords must meet the following criteria:

(a) contain at least 8 characters;

(b) not match previous passwords, the user's login, or common name;

(c) must be changed whenever an account compromise is suspected or assumed.

2.6.5 Vendor will maintain and enforce "account lockout" by disabling accounts with access to Extreme Information when an account exceeds more than ten (10) consecutive incorrect password attempts.

2.6.7 If additional physical access controls are requested in writing by Extreme, Vendor will implement and use those secure physical access control measures.

2.6.8 Vendor will regularly review access logs for signs of malicious behavior or unauthorized access.

2.7 Vendor will maintain and enforce an information and network security policy for employees, subcontractors, agents, and contractors that meets the standards set out in this policy, including methods to detect and log policy violations. Upon request by Extreme, Vendor will provide Extreme with information on violations of Vendor's information and network security policy, even if it does not constitute a Security Breach.

2.8 Vendor will not subcontract or delegate any of its obligations under this Addendum to any subcontractors, affiliates, or delegates ("**Subcontractors**") unless such Subcontractors have been duly qualified by Vendor and in any event, notwithstanding the existence or terms of any subcontract or delegation, Vendor will remain responsible for the full performance of its obligations under this Addendum. Vendor will be responsible for all acts, omissions, negligence and misconduct of its Subcontractors and employees.

2.9 Vendor will ensure that any access from outside protected corporate or production environments to systems holding Extreme Information or Vendor's corporate or development workstation networks requires multi-factor authentication (*i.e.*, requires at least two separate factors for identifying users).

2.10 Extreme may grant Vendor access to Extreme Information via web portals or other non-public websites or extranet services on Extreme's website or system (each, an "**Extranet**"). If Extreme permits Vendor to access any Extreme Information using an Extranet, Vendor must comply with the following requirements:

2.10.1 Vendor will ensure that Vendor personnel use only the Extranet account(s) designated for each individual by Extreme and will require Vendor personnel to keep their access credentials confidential.

2.10.2 Vendor will access the Extranet only through computing or processing systems or applications running operating systems managed by Vendor and that include: (i) system network firewalls in accordance with Section 2.5.1; (ii) centralized patch management in compliance with Section 2.5.2; (iii) operating system appropriate anti-malware software in accordance with Section 2.5.3; and (iv) for portable devices, full disk encryption.

2.10.3 Unless approved in advance in writing by Extreme, Vendor will not download, mirror or permanently store any Extreme Information from any Extranet on any medium, including any machines, devices or servers.

2.10.4 Vendor will terminate the account of each of Vendor's employees/contractors/subcontractors and notify Extreme no later than 24 hours after any specific Vendor personnel who has been authorized to access any Extranet (a) no longer needs access to Extreme Information or (b) no longer qualifies as Vendor personnel (*i.e.*, the personnel leaves Vendor's employment).

2.11 Third-Party Systems.

2.11.1 Vendor will give Extreme prior notice and obtain Extreme's prior written approval before it uses any third-party system that stores or may otherwise have access to Extreme Information, unless a) the data is encrypted in accordance with this Addendum, and b) the third-party system will not have access to the decryption key or unencrypted "plain text" versions of the data. Extreme reserves the right to require an Extreme security review (in accordance with Section 3 (Security Review)) of the third-party system before giving approval.

2.11.2 If Vendor uses any third-party systems that store or otherwise may access unencrypted Extreme Information, Vendor must perform a security review of the third-party systems and their security controls and will provide Extreme periodic reporting about the third-party system's security controls in the format requested by Extreme (*e.g.*, SAS 70 or other recognized industry-standard report approved by Extreme).

3. **SECURITY REVIEW**.

3.1 Extreme reserves the right to periodically request Vendor to complete a new Extreme risk assessment questionnaire.

3.2 Upon Extreme's written request, Vendor will certify in writing to Extreme that it is in compliance with this Addendum.

3.3 Extreme reserves the right to periodically review the security of systems that Vendor uses to process Extreme Information. Vendor will cooperate and provide Extreme with all required information, which information shall be deemed to be Vendor's Confidential Information, within a reasonable time frame but no more than 20 calendar days from the date of Extreme's written request.

3.4 If any security review identifies any deficiencies, Vendor will, at its sole cost and expense take all reasonable actions necessary to remediate those deficiencies within an agreed upon timeframe.

4. **SECURITY BREACH INCIDENTS**.

4.1 Vendor shall:

4.1.1 provide Extreme with the name(s) and contact information for one or more employee(s) of Vendor who shall serve as Extreme's primary security contact(s) and who shall be available to assist Extreme 24x7, seven days a week as a contact in resolving obligations associated with a Security Breach;

4.1.2 notify Extreme of a Security Breach as soon as practicable, but no later than 48 hours after Vendor becomes aware of it; and

4.1.3 notify Extreme of any Security Breaches by email to EXTR-ThirdParties-Incidents@extremenetworks.com, and second copy to Vendor's primary business contact with Extreme.

4.2 Vendor will take reasonable steps, at Vendor's expense, to remedy each Security Breach in a timely manner and prevent any further Security Breach, in accordance with applicable privacy laws, regulations, and standards. Vendor shall reimburse Extreme for actual costs incurred by Extreme in responding to, and mitigating damages caused by, any Security Breach, including all reasonable costs of notice and/or remediation. If applicable, such costs reimbursed by Vendor to Extreme shall include the costs incurred by Extreme in providing individuals affected by the Security Breach with reissued payment cards, complimentary access for one (1) year credit monitoring services, credit protection services, credit fraud alerts and/or similar services, which Extreme, in its sole discretion, deems necessary to protect such affected individuals in light of the risks posed by the Security Breach.

4.3 Vendor shall provide Extreme with written details regarding each Security Breach, including the type of data that was the subject of the Security Breach and (to the extent known to the Vendor) the identity of each affected person, as soon as such information can be collected or otherwise becomes available, as well as all other information and cooperation that Extreme may reasonably request relating to the Security Breach. Vendor agrees to cooperate at its own expense with Extreme in any litigation or other formal action deemed reasonably necessary by Extreme to protect its rights relating to the use, disclosure, protection and maintenance of Extreme Information.

4.4 Vendor agrees not to notify any regulatory authority or any customer on behalf of Extreme unless Extreme specifically requests in writing that Vendor do so, and Extreme reserves the right to review and approve the form and content of any notification before it is provided to any party.

4.5 Vendor shall not issue, publish or make available to any third party any press release or other communication concerning a Security Breach without Extreme's prior approval.

4.6 Unless prohibited by law, Vendor will inform Extreme within 24 hours when Extreme Information or other data is being sought in response to legal process or by applicable law.

5. DESTRUCTION OR RETURN OF EXTREME INFORMATION.

5.1 At any time during the term of the Services Agreement at Extreme's request or within thirty (30) days following the termination or expiration of the Services Agreement for any reason, Vendor shall, and shall instruct all Authorized Persons to, promptly return to Extreme all copies, whether written, electronic or other form or media, of Extreme Information in its possession or the possession of such Authorized Persons, or security dispose of all such copies and certify in writing to Extreme that such Extreme Information has been returned to Extreme or disposed of securely. If requested by Extreme, Vendor will certify in writing that all Extreme Information has been destroyed. Vendor shall comply with all reasonable directions provided by Extreme with respect to the return or disposal of Extreme Information.

5.2 If Vendor is required by law to retain archival copies of Extreme Information for tax or similar regulatory purposes, this archived Extreme Information must be stored in one of the following ways:

5.2.1 As a "cold" or offline (*i.e.*, not available for immediate or interactive use) backup stored in a physically secure facility; or

5.2.2 Encrypted, where the system hosting or storing the encrypted file(s) does not have access to a copy of the key(s) used for encryption.

5.2.3 If Vendor performs a "recovery" (*i.e.*, reverting to a backup) for the purpose of disaster recovery, Vendor will have and maintain a process that ensures that all Extreme Information that is required to be deleted pursuant to the Agreement or this Addendum will be re-deleted or overwritten from the recovered data in accordance with this Section 5 within 24 hours after recovery occurs. If Vendor performs a recovery for any purpose, no Extreme Information may be recovered to any third-party system or network without Extreme's prior written approval. Extreme reserves the right to require an Extreme security review (in accordance with Section 3 (Security Review)) of the third-party system or network before permitting recovery of any Extreme Information to any third-party system or network.

5.2.4 All Extreme Information deleted by Vendor will be deleted in accordance with the NIST Special Publication 800-88 Revision 1, Guidelines for Media Sanitation December 18, 2014 (available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf), or through degaussing of magnetic media in an electromagnetic flux field of 5000+ GER, or by shredding or mechanical disintegration, or such other standards Extreme may require based on the classification and sensitivity of the Extreme Information. With respect to Extreme Information encrypted in compliance with this Addendum, this deletion may be done by permanently and securely deleting all copies of the keys used for encryption.

5.2.5 Before disposing in any manner of any hardware, software, or any other media that contains, or has at any time contained, Extreme Information, Vendor will perform a complete forensic destruction of the hardware, software or other media so that none of the Extreme Information can be recovered or retrieved in any form.

5.2.6 Vendor will not sell, resell, donate, refurbish, or otherwise transfer (including any sale or transfer of any such hardware, software, or other media, any disposition in connection with any liquidation of Vendor's business, or any other disposition) any hardware, software or other media that contains Extreme Information that has not been forensically destroyed by Vendor.

6. **EQUITABLE RELIEF.**

Vendor acknowledges that any breach of its covenants or obligations set forth in this Exhibit 2 may cause Extreme irreparable harm for which monetary damages would not be adequate compensation and agrees that, in the event of such breach or threatened breach, Extreme is entitled to seek equitable relief, including a restraining order, injunctive relief, specific performance and any other relief that may be available from any court, in addition to any other remedy to which Extreme may be entitled at law or in equity. Such remedies shall not be deemed to be exclusive but shall be in addition to all other remedies available at law or in equity.

7. **CYBER INSURANCE.**

During the Term of the Services Agreement and at all times when Vendor or its subcontractors control, possess, store, hosts, transmits or processes Extreme Information, Vendor shall, at its own expense, provide and keep in full force without interruption, liability insurance covering liabilities for financial losses resulting from acts, errors or omissions, in connection with rendering the Services, and which covers:

7.1.1 violation or infringement of any right of privacy, including breach of security and breach of applicable privacy laws/regulations globally;

7.1.2 data theft, damage, unauthorized disclosure, destruction, or corruption, including without limitation, unauthorized access, unauthorized use, identity theft, theft of personally data or confidential corporate information in whatever form, transmission of a computer virus or other type of malicious code or participation in a denial of service attack on third party computer systems;

7.1.3 loss or denial of service;

7.1.4 no cyber terrorism exclusion; and

7.1.5 with a minimum limit of $5,000,000 for each and every claim and in the aggregate.

-Exhibit 3 follows this page-

EXHIBIT 3

CONTROLLER-PROCESSOR TERMS

1. DATA PROTECTION.

1.1. In this Exhibit 3, the terms "process", "data controller", "data processor", "data subject" and "supervisory authority" shall have the meanings set out in the GDPR or corollary in the applicable Data Protection Law.

1.2. Vendor is appointed by Extreme for the duration of the term of the Services Agreement to process Personal Data on behalf of Extreme as is necessary to provide the Services and in accordance with such other written instructions as Extreme may issue from time to time.

1.3. Extreme warrants that it is the data controller in respect of the Personal Data or is authorized by the data controller to issue instructions to the Vendor under this Addendum in respect of such Personal Data.

1.4. Each party shall comply with its obligations under the Data Protection Law in respect of any Personal Data it processes under or in relation to the Services Agreement. Without prejudice to the foregoing, Vendor shall not process Personal Data in a manner that will or is likely to result in Extreme breaching its obligations under the Data Protection Law.

1.5. The categories of Extreme Personal Data to be processed by Vendor and the processing activities to be performed under the Services Agreement and this Addendum are set out in Schedule 1.

1.6. Vendor warrants and represents in respect of all Personal Data that at all times it shall:

1.6.1 only process Personal Data in accordance with this Addendum, and the documented instructions given from time to time by Extreme, including with regard to transfers, unless required to do otherwise by applicable law (in which event, Vendor shall inform Extreme of the legal requirement before processing Extreme Personal Data other than in accordance with Extreme's instructions, unless that same law prohibits the Vendor from doing so on important grounds of public interest);

1.6.2 implement appropriate technical and organisational measures to protect any Personal Data processed by it against unauthorised and unlawful processing and against accidental loss, destruction, disclosure, damage or alteration, as set forth in Exhibit 2.

1.6.3 not publish, disclose or divulge (and ensure that its personnel do not publish, disclose or divulge) any Personal Data to any third party unless Extreme has given its prior written consent;

1.6.4 ensure that only such of its Authorized Persons who may be required by the Vendor to assist it in meeting its obligations under the Services Agreement and this Addendum will have access to Personal Data and that such personnel are bound by appropriate obligations of confidentiality, and take all reasonable steps in accordance with best industry practice to ensure the reliability of such personnel;

1.6.5 inform Extreme promptly, and in any event within two (2) business days, of any enquiry or complaint received from a data subject or supervisory authority relating to Personal Data;

1.6.6 at no additional cost, provide full cooperation and assistance to Extreme as Extreme may require to allow Extreme to comply with its obligations under the Data Protection Law, including in relation to data security; data breach notification; data protection impact assessments; prior consultation with supervisory authorities; the fulfilment of data subject's rights; and any enquiry, notice or investigation by a supervisory authority;

1.6.7 at the request and option of Extreme (whether during or following termination of the Services Agreement), promptly, and as specified by Extreme, return or destroy all Extreme Personal Data in the possession or control of the Vendor; and

1.6.8 refrain from selling any Extreme Personal Data.

1.7 Subject to any provisions of this Addendum to the contrary, the Vendor shall not appoint any third party to process Extreme Personal Data ("**Subprocessor**") without Extreme's prior written consent, and subject in all cases to the Vendor:

1.7.1 providing reasonable prior notice to Extreme of the identity and location of the Subprocessor and a description of the intended processing to be carried out by the Subprocessor to enable Extreme to evaluate any potential risks to Extreme Personal Data; and

1.7.2 imposing legally binding contract terms on the Subprocessor that are the same as those contained in this Exhibit 3.

1.8 The Vendor acknowledges and agrees that it shall remain liable to Extreme for a breach of the terms of this Exhibit 3 by a Subprocessor and other subsequent third-party processors appointed by it.

2. SECURITY BREACHES.

2.1 The Vendor shall follow the security breach obligations set forth in Exhibit 2 to this Addendum.

2.2 The Vendor shall make available to Extreme all information necessary to demonstrate compliance with this Exhibit 3 and allow for and contribute to audits, including physical

inspections, conducted by the Extreme or its representatives bound by appropriate obligations of confidentiality.

3. DATA TRANSFERS.

3.1 The Vendor shall ensure that no Extreme Personal Data from data subjects located in any jurisdiction that restricts the transfer of Personal Data of its residents to areas outside its jurisdiction or region is transferred to or processed outside of such jurisdiction or region, without the express prior written consent of Extreme.

3.2 To the extent that consent is granted, the terms of the transfer shall be governed by the EU Standard Contractual Clauses for the transfer of Personal Data to processors attached as Schedule 2 or other similar transfer mechanism, which are hereby incorporated into this Addendum.

3.3 If, for whatever reason, the transfer of Extreme Personal Data as set forth in this Exhibit 3 ceases to be lawful, the Vendor shall either:

3.3.1 with Extreme's consent, implement an alternative lawful transfer mechanism; or

3.3.2 allow Extreme to terminate the Services Agreement at no additional cost to Extreme.

-Schedule 1 follows this page-

Schedule 1: Description of Personal Data Processing

The data processing activities carried out by the Vendor under the Services Agreement and this Addendum may be described as follows:

1. **Subject matter**

   The subject matter of the processing of the Personal Data is set out in the Services Agreement and this Addendum.

2. **Duration**

   During the term of the Services Agreement (including any Statements of Work thereunder) executed by the Parties.

3. **Nature and purpose**

   In the performance of Services under the Service Agreement, Vendor may from time to time perform data processing activities which may include, without limitation: (i) use of Personal Data to provide the Services; (ii) collecting, recording, storing, structuring, modifying, adapting, altering or destroying the Personal Data of a data subject; and (iii) execution of instructions of Extreme in accordance with the Services Agreement and this Addendum.

4. **Data categories**

   - Names
   - Addresses, and other contact details
   - Phone number
   - Email
   - Age and/or date of birth
   - Gender
   - National identification number (i.e. SSN)
   - Family and social circumstances such as marital status or dependent details
   - Employment and other records that include education and training details, which may include academic records, qualifications, skills, training records, professional expertise, and/or work experience
   - Financial details such as bank account information or details, and information pertaining to salary, bonus and/or equity
   - IP address
   - MAC address

5. **Data subjects**

- Extreme employees
- Extreme contractors
- Extreme candidates for employment
- Extreme customers
- Extreme business partners (including suppliers, vendors, consultants, distributors, resellers)

-Schedule 2 follows this page-

Schedule 2 - Standard Contractual Clauses

ANNEX

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.

[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.

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) 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 the 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 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.

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.

[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.

(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

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

(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.

(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

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 sub-processor 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) 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];

(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.

[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.

(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 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 ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller (where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

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 achieved 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):

1.Name: Extreme Networks, Inc.

Address: 2121 RDU Center Drive, Suite #300, Morrisville, NC 27560

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

Activities relevant to the data transferred under these Clauses: …Data is transferred pursuant to Extreme's purchase of the Services.

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

…

2. Data importer(s):

1.Name: Vendor

Address: …Vendor's address identified in the Services Agreement and/or on the face of the purchase order.

Contact person's name, position and contact details: … Contact details identified in the Services Agreement and/or on the face of the purchase order.

Activities relevant to the data transferred under these Clauses: The provisioning of the Services to Extreme pursuant to the Services Agreement and subject to this Agreement.

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

…

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

Categories of data subjects whose personal data is transferred

… **[See Schedule 1: Description of Personal Data Processing above]**

Categories of personal data transferred

… **[See Schedule 1: Description of Personal Data Processing above]**

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.

… **[See Schedule 1: Description of Personal Data Processing above]**

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

… **[on a continuous basis]**

Nature of the processing

… **[See Schedule 1: Description of Personal Data Processing above]**

Purpose(s) of the data transfer and further processing

… **[See Schedule 1: Description of Personal Data Processing above]**

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

… **[for the retention period as set forth in this Agreement]**

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

… **[such transfers are subject to the terms and conditions of this Agreement]**

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer controller to processor

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

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.

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.

See Exhibit 2 to the Addendum

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.

See Exhibit 2 to the Addendum

-End of Agreement-