Data Privacy Addendum ("DPA")

This Data Privacy Addendum ("DPA") is by and between Arista Networks, Inc. and Arista Networks Ltd. (collectively, "**Arista**"), with places of business at 5453 Great America Parkway, Santa Clara, California, 95054 and 3130 Atlantic Avenue, Westpark Business Campus, Shannon, Co. Clare, Ireland, respectively, and You, the customer ("You" or "**Customer**") when You subscribe to any of Arista's Cloud Services memorialized in an agreement between the parties, which may be defined as a cloud subscription agreement or master services agreement and You have not signed separate data privacy terms with Arista.

1. A new Data Privacy Exhibit, as set forth below, is added to the Agreement and forms an integral part thereof.

2. To the extent that any Agreement contains any terms or conditions that are inconsistent with the terms of the Data Privacy Exhibit, the terms of the attached Data Privacy Exhibit shall prevail. All other provisions of any Agreement shall remain in full force and effect.

DATA PRIVACY EXHIBIT

In delivering the services under the Agreement, Arista and its worldwide corporate entities may process Personal Data provided by or on behalf of Customer. Arista takes the protection and privacy of this data seriously, will ensure that its partners protect this data with at least the same level of care, and will not use the data other than as described herein.

1. DEFINITIONS

1.1 **"Applicable Privacy Law(s)"** means all worldwide data protection and privacy laws and regulations either now in effect or that become effective during the term of the Agreement applicable to the Personal Data in question, including, where applicable, the EU and UK general Data Protection Regulation (collectively, the "**GDPR**") and the 2020 California Privacy Rights Act (**"CPRA"**).

1.2 **"Authorized Persons"** means any person who processes Personal Data on Arista's behalf, including Arista's employees, officers, partners, principals, contractors and Subcontractors.

1.3 **"Cloud Services"** means the Subscription Services described in the Agreement and to which Customer subscribes.

1.4 **"Customer Employee Data"** means any Personal Data of an employee, officer, partner, principal, contractor, intern, or other member of Customer.

1.5 **"Personal Data"** means information relating to an identified or identifiable natural person ("**data subject**"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to their physical, physiological, genetic, mental, economic, cultural or social identity. For the avoidance of doubt, Personal Data includes personally identifiable information.

1.6 **"Security Incident"** means any unauthorized or unlawful breach of security leading to the accidental or unlawful destruction loss, alteration, unauthorized disclosure or access to Personal Data.

1.7 **"Service Personal Data"** means any Personal Data that Customer or Customer's end users process through the Cloud Services.

1.8 **"Subcontractor"** means any third party (including any Arista Entity) engaged to process any Personal Data relating to this DPA and/or the agreements between Arista and Customer; Subcontractor is equivalent to "sub-processor" under the EU SCCs (as defined below).

1.9 **"Arista Entity"** means any entity that Arista Networks, Inc. controls (directly or indirectly), where "control" means at least fifty percent (50%) ownership of the outstanding shares of the entity, or the ability to direct the management of the entity by contract or otherwise.

1.10 The terms **"Data Controller"/ "Controller"/ "Business," "Data Processor"/ "Processor"/ "Service Provider,"** and **"processing,"** have the meanings given to them in Applicable Privacy Laws. If and to the extent that Applicable Privacy Laws do not define such terms, then the definitions given in Applicable Privacy Laws will apply.

2. ROLE AND SCOPE OF PROCESSING

2.1 Arista and Customer will comply with all applicable requirements of the Applicable Privacy Laws. Arista shall process Service Personal Data through the Cloud Services only as a Processor acting on behalf of Customer (whether as Controller or itself a Processor on behalf of third party Controllers). Customer has ensured and will continue to ensure that it has the rights to transfer both the Service Personal Data and any relevant Customer Employee Data to Arista for the duration and purposes of the Agreement.

2.2 Arista will at all times:

a) process the Personal Data only for the purpose of (1) providing the Services to Customer under the Agreement; (2) contacting Customer regarding any support for such Services or the pending or potential sale or license of Arista's products and Services; or (3) improving the Services, each of the forgoing

items (1)-(3) in accordance with Customer's documented instructions including this DPA (except where otherwise required by applicable law);

b) not process the Personal Data for its own purposes or those of any third party; for the avoidance of doubt, Arista shall only collect, record, store, retain, use, access, disclose, transmit, and transfer Personal Data in accordance with the instructions of and on behalf of Customer, as necessary to carry out the purposes of the Agreement in accordance with **Annex A** or as otherwise authorized by Customer in writing and for no other purpose. Arista shall not engage in the sale (i.e., “share” under certain Applicable Privacy Laws) of Personal Data, nor shall Arista combine Personal Data of Customer with any other Personal Data held by or accessible to Arista to provide services to any other entity or customer of Customer;

c) if Arista is required by any applicable law to process such Personal Data for other purposes, promptly notify Customer of such other purposes before performing the processing required, unless such law prohibits notifying Customer;

d) ensure that it has in place appropriate technical and organizational measures, to protect against unauthorized or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data, appropriate to the harm that might result from the unauthorized or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures (those measures may include, where appropriate, pseudonymisation and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of its systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the technical and organizational measures adopted by it);

e) ensure that all Arista personnel who have access to and/or process Personal Data are obliged to keep the Personal Data confidential;

f) assist Customer, at Customer's cost, in responding to any request from a Data Subject and in ensuring Customer's compliance with its obligations under the Applicable Privacy Laws with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators;

g) at the written direction of Customer, delete or return Personal Data and copies thereof to Customer on termination of the Agreement unless required by Applicable Laws to store the Personal Data;

h) notify Customer if, in Arista’s assessment, any of Customer’s instructions infringe applicable law, including but not limited to Applicable Privacy Laws and, in the event that Arista determines that it can no longer meet its

obligations under this DPA, Arista shall notify Customer promptly after making such a determination.

i) maintain complete and accurate records and information to demonstrate its compliance with this DPA and allow for audits by Customer; and

j) comply with all reasonable requests of Customer resulting from any such audit.

2.3 Customer recognizes that it is in its best interest that Arista continue to update and improve the Services for Customer. While recognizing that Arista shall be in sole control of the priority and direction of such updates, improvements, and new features, Customer instructs Arista to use anonymized or pseudo-anonymized versions of such Personal Data, when useful, to help such advancement of the Services.

3. INTERNATIONAL TRANSFER

3.1 Arista and the Arista Entities have a global presence and employ cloud service providers to manage data (pursuant to Section 4 below). Customer understands that Arista cannot guarantee that Personal Data given to it will reside in only one country and expressly authorizes Arista to transfer the Personal Data to locations inside and outside of the European Economic Area ("**EEA**") and United Kingdom ("**UK**") in compliance with any restrictions in law or as set forth herein.

3.2 EU Standard Contractual Clauses. As applicable to the Agreement and to the extent required by Applicable Privacy Laws, the parties agree that the clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("**EU SCCs**") will apply to Personal Data that is transferred under the Agreement from the EEA or Switzerland, either directly or via onward transfer, to any country or recipient outside the EEA or Switzerland that is not recognized by the European Commission (or, in the case of transfers from Switzerland, the competent authority for Switzerland) as providing an adequate level of protection for Personal Data ("**Restricted Transfer**"). For data transfers from the EEA that are subject to the EU SCCs, the EU SCCs, Module 2 (Controller to Processor), will be deemed entered into (and incorporated into this Addendum by this reference) and completed as follows:

a) In Clause 7, the optional docking clause will not apply;

b) In Clause 9, Option 2 will apply and the time period for notice of Subcontractor changes will be as set forth in Section 3 of this Addendum;

c) In Clause 11, the optional redress language will not apply;

d) In Clause 13(a), all three options may be retained and apply, depending on the circumstances, and as relevant where the transfer falls within the territorial scope of the Regulation (EU) 2016/679;

e) In Clause 17, Option 1 will apply and the EU SCCs will be governed by Irish law;

f) In Clause 18(b), disputes will be resolved before the courts of Ireland; and

g) **Annex A** (Data Processing Description) of this Addendum serves as Annex I of the EU SCCs; **Annex B** (Technical and Organizational Security Measures) of this Addendum serves as Annex II of the EU SCCs and **Annex C** (Approved Subcontractor) serves as Annex III of the EU SCCs.

3.3 UK Addendum. As applicable to the Agreement and in relation to Personal Data that is protected by the UK GDPR, the UK Addendum to the EU Standard Contractual Clauses ("**UK Addendum**") shall apply. To the extent that the UK Addendum applies, Annexes A, B, and C of this Addendum shall also apply. For data transfers from the United Kingdom that are subject to the UK Addendum, the UK Addendum will be deemed entered into (and incorporated into this Addendum by this reference) and completed as follows:

a) For Table One, the details as set out in **Annex A** of this Addendum shall apply.

b) For Table Two, the check-box referring to the following shall apply: "the Approved EU SCCs, including the Appendix Information and with only the modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of the UK Addendum."

Within the table, Module 2 shall apply and shall be filled out in the same way as the EU SCCs as filled out in Section 8.4 (EU Standard Contractual Clauses) above.

c) For Table Three, the following shall apply to the referenced columns: **Annex A** (Data Processing Description) of this Addendum shall apply to the columns entitled Annex IA and Annex IB; **Annex B** (Technical and Organizational Security Measures) of this Addendum shall apply to the column entitled Annex II; and **Annex C** (Approved Subcontractor) shall apply to the column entitled Annex III.

d) For Table Four, data exporter and data importer shall have the right to terminate this Addendum.

3.4 Additionally, Arista enters into the EU SCCs with Customer subject to the following additional terms. The Parties agree that this section is not intended to amend or modify the EU SCCs but represent agreed processes for complying therewith.

a) Processing Instructions. Pursuant to Clause 4(b) of the EU SCCs, Customer acknowledges and agrees that the provisions of the Agreement and further contained herein comprise the instructions for and approval to process personal data.

b) Appointment of new Sub-processors and List of current Sub-processors. Pursuant to Clause 5(h) of the EU SCCs, Customer acknowledges and expressly agrees that (a) any Arista Entity may be retained as a Subcontractor; and (b) any Arista Entity may engage third-party Subcontractor in connection with the provision of Arista products and Services as set forth in Section 4 below.

c) In the event of any conflict or inconsistency between the body of this DPA and the EU SCCs, the EU SCCs shall prevail.

3.5 With respect to the international transfer of data out of the EU, Arista reserves the right to switch to another transfer mechanism approved by the EU Commission or UK Information Commissioner's Office, as applicable, provided that it does not materially reduce the protections provided herein.

4. SUBPROCESSING

4.1 Customer agrees that Arista has general authorization to utilize affiliates and subsidiaries, agents, subcontractors, or other third parties to assist Arista in providing the Services under the Agreement, provided that:

a) Arista imposes substantially similar or more stringent data protection terms on any Subcontractor it engages as contained in this DPA; and

b) Arista shall be responsible for the actions of its Subcontractors in accordance with the terms of the Agreement.

See **Annex C** for the current list of Arista Subprocessors - which may be updated from time to time**.**

4.2 In the event, Arista decides to engage any additional Subcontractor, Arista will notify, through the website listed in **Annex C** and as Customer subscribes thereto, Customer in advance of providing the Subcontractor access to Customer Personal Data. If Customer objects to the engagement of any Subcontractor within fifteen (15) days of such notification on data protection grounds, then either Arista will not engage the Subcontractor to process the Personal Data controlled by Customer or Arista may elect to suspend or terminate the processing of Personal Data under the Agreement without penalty unless and until Customer and Arista reach an agreement.

4.3 Customer agrees that any Arista Entity may process, subprocess, or engage an approved Subcontractor to process or subprocess Customer's Personal Data in

accordance with the terms herein. In furtherance thereof, Arista may transfer such Personal Data to any other Arista Entity.

5. DATA SUBJECTS AND COOPERATION

5.1 Arista shall reasonably cooperate to enable Customer to respond to any requests, complaints or other communications from Data Subjects and regulatory or judicial bodies relating to the processing of Personal Data under the Agreement, including requests from Data Subjects seeking to exercise their rights under Applicable Privacy Laws. In the event that any request, complaint or communication is made directly to Arista regarding Service Personal Data, Arista shall promptly pass this onto Customer and shall not respond to such communication without Customer's express authorization. Any such assistance will only be required to the extent Customer cannot otherwise address the relevant request on its own and at Customer's sole cost and expense.

5.2 If Arista receives a subpoena, court order, warrant or other legal demand from a third party (including law enforcement or other public or judicial authorities) seeking the disclosure of Personal Data, Arista shall not disclose any information but shall notify Customer in writing of such request, and reasonably cooperate with Customer if it wishes to limit, challenge or protect against such disclosure, to the extent permitted by applicable laws and at Customer's cost and expense. If Arista is not permitted under law to notify Customer, Arista will (1) seek waiver of any such requirement if possible; (2) require formal requests pursuant to legal process (such as a subpoena or court order); (3) analyze the lawfulness of any such request; and (4) challenge requests Arista deems, in its sole discretion, to be unlawful.

5.3 To the extent Arista is required under Article 28(3) GDPR, Arista will reasonably assist Customer (or its third party Controller) to comply with Articles 35 & 36 GDPR or provide similar assistance to the extent required by Applicable Privacy Law. Such assistance will only be required to the extent Customer cannot otherwise address the relevant request on its own and at Customer's sole cost and expense.

6. DATA ACCESS & SECURITY MEASURES

6.1 Arista shall take steps to confirm that any Authorized Person is subject to a strict duty of confidentiality (whether a contractual or statutory duty) and that they process the Personal Data only for the purpose of delivering the Services under the Agreement to Arista.

6.2 Arista will implement and maintain all appropriate technical and organizational security measures to protect from Security Incidents and to preserve the security, integrity and confidentiality of Personal Data (**"Security Measures"**). Such measures shall have regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as to the

likelihood and severity of the risk to the rights and freedoms of natural persons. At a minimum, Arista agrees to the Security Measures identified at **Annex B.**

6.3 Arista Cloud Services may be hosted by Subcontractors in their data centers. In such cases, there is a shared responsibility model (**"SRM"**) for cloud security. In this model, the Subcontractor(s) manage the security of the data centers, including physical security, environmental protection, administrative controls, technical controls, and redundant infrastructure. Arista inherits data center security controls from the Subcontractor(s) and does not have the ability to influence their implementation or the ability to monitor or audit them. In accordance with the relevant SRM, Arista manages security of the Cloud Services application and application data, including boundary protection, host firewalls, application hardening, vulnerability assessment, data encryption, logical access control, availability monitoring, change management, and disaster recovery. Arista performs regular monitoring and evaluation of its security.

7. SECURITY INCIDENTS

7.1 In the event of a Security Incident, Arista shall promptly inform Customer of any actual loss or compromise of Customer Personal Data and provide written details of the Security Incident, including the type of data affected and the identity of affected person(s) as soon as such information becomes known or available to Arista.

7.2 Furthermore, in the event of a Security Incident, Arista shall:

a) provide timely information and cooperation as reasonably needed for Customer to fulfill Customer's data breach reporting obligations under Applicable Privacy Laws;

b) take such measures and actions as are appropriate to remedy or mitigate the effects of the Security Incident; and

c) keep Customer up-to-date about all developments in connection with the Security Incident.

7.3 The content and provision of any notification, public/regulatory communication or press release concerning the Security Incident shall be solely at Arista's discretion, except as otherwise required by applicable laws.

8. SECURITY REPORTS

8.1 Upon request, Arista shall provide copies of relevant documentation reasonably required by Arista to verify Arista's compliance with this DPA. If additional audits are required by Applicable Privacy Law, Arista shall cooperate with Customer to determine the scope of any such audit, which shall be conducted at the expense of Customer.

9. DELETION & RETURN

9.1 Upon Customer's reasonable request, or upon termination or expiry of this DPA, Arista shall destroy or return to Customer all Service Personal Data (including copies) in its possession or control (including any Service Personal Data processed by its Subcontractors). This requirement shall not apply to the extent that Arista is required by any applicable law to retain some or all of the Service Personal Data, in which event Arista shall isolate and protect the Service Personal Data from any further processing except to the extent required by such law.

10. GENERAL

10.1 The term of this DPA and the obligations placed upon Arista thereunder shall survive so long as Arista and/or its Subcontractors processes Personal Data on behalf of Customer.

10.2 This DPA may be modified unilaterally by Arista, provided that Arista notifies Customer and does not materially lower the security and data processing protections for Customer herein; otherwise this DPA may not be modified except by a subsequent written instrument signed or otherwise agreed to by both parties.

10.3 If any part of this DPA is held unenforceable, the validity of all remaining parts will not be affected.

10.4 In the event of any conflict between this DPA, the EU SCCs and UK Addendum, as applicable, and any data privacy provisions set out in any Agreement, the parties agree that the terms of the EU SCCs and UK Addendum shall prevail.

ANNEX A – DATA PROCESSING DESCRIPTION

A. LIST OF PARTIES

MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor

Data exporter(s):
1. Name: **Customer as set forth in the DPA**
   Address:
   Contact person's name, position and contact details:
   Activities relevant to the data transferred under these Clauses:

   Signature and date: …

   Role (controller/processor): controller or processor

Data importer(s):
1. Name: **Arista**
   Address:
   Contact person's name, position and contact details:
   Activities relevant to the data transferred under these Clauses:

   Signature and date: …

   Role (controller/processor): processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

1) Controller's employees and/or controller's end users of the Products and Services of the Agreement

Categories of personal data transferred

1) Contact Information, user device IDs and addresses, and location data as determined by Controller through the Services and their configurations

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

1) N/A

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

ongoing/continuous

Nature of the processing

Storage and evaluation to provide the Services as set forth in the Agreement

Purpose(s) of the data transfer and further processing

To provide the Services as set forth in the Agreement

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

Duration of the Agreement and any subsequent similar agreement

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

As described in the DPA and Agreement

C. COMPETENT SUPERVISORY AUTHORITY

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

The Data Protection Commission of Ireland

Annex B

Technical and Organizational Security Measures

This Annex B sets out a description of the minimum technical and organizational security measures that Arista implements.

Arista takes information security seriously and this approach is followed through in its processing and transfers of personal data. This information security overview applies to Arista's corporate controls for safeguarding personal data which is processed and transferred amongst Arista's group companies. Arista's information security program enables the workforce to understand their responsibilities. Some customer solutions may have alternate safeguards outlined in the applicable statement of work as agreed with each customer.

Security Practices

Arista has implemented corporate information security practices and standards that are designed to safeguard Arista's corporate environment and to address business objectives across the following areas:

1. information security
2. system and asset management
3. development, and
4. governance.

These practices and standards are approved by Arista's executive management and are periodically reviewed and updated where necessary.

Arista shall maintain an appropriate data privacy and information security program, including policies and procedures for physical and logical access restrictions, data classification, access rights, credentialing programs, record retention, data privacy, information security and the treatment of personal data and sensitive personal data throughout its lifecycle. Key policies should be reviewed at least annually.

Organizational Security

It is the responsibility of the individuals across Arista's organization to comply with these practices and standards. To facilitate the corporate adherence to these practices and standards, Arista's Information Security ("**IS**") function is responsible for the following activities:

1. **Security strategy** – the IS function drives Arista's security direction. The IS function works to ensure compliance with security related policies, standards and regulations, and to raise awareness and provide education to users. The IS

function also carries out risk assessments and risk management activities, and manages contract security requirements.

2. **Security engineering** – the IS function manages testing, design and implementation of security solutions to enable adoption of security controls across the environment.

3. **Security operations** – the IS function manages support of implemented security solutions, monitors and scans the environment and assets, and manages incident response.

4. **Forensic investigations** – the IS function works with Security Operations, Legal, Global Privacy Office and Human Resources to carry out investigations, including eDiscovery and eForensics.

5. **Security consulting and testing** – the IS function works with software developers on developing security best practices, consults on application development and architecture for software projects, and carries out assurance testing.

Asset Classification and Control

Arista's practice is to track and manage key information and physical, software and logical assets. Examples of the assets that Arista might track include:

- information assets, such as identified databases, disaster recovery plans, business continuity plans, data classification, archived information
- software assets, such as identified applications and system software
- physical assets, such as identified servers, desktops/laptops, backup/archival tapes, printers and communications equipment.

The assets are classified based on business criticality to determine confidentiality requirements. Industry guidance for handling personal data provides the framework for technical, organizational and physical safeguards. These safeguards may include controls such as access management, encryption, logging and monitoring, and data destruction.

Employee Screening, Training and Security

1. **Screening/background checks:** Where reasonably practicable and appropriate, as part of the employment/recruitment process, Arista shall perform screening/background checks on employees (which shall vary from country to country based on local laws and regulations), where such employees will have access to Arista's networks, systems or facilities.

2. **Identification:** Arista shall require all employees to provide proof of identification and any additional documentation that may be required based on the country of hire or if required by other Arista entities or customers for whom the employee is providing services.

3. **Training:** Arista's annual compliance training program includes a requirement for employees to complete a data protection and information security awareness course and pass an assessment at the end of the course. The security awareness course may also provide materials specific to certain job functions.

4. **Confidentiality:** Arista shall ensure its employees are legally bound to protect and maintain the confidentiality of any personal data they handle pursuant to standard agreements.

Physical Access Controls and Environmental Security

1. **Physical Security Program:** Arista shall use a number of technological and operational approaches in its physical security program to mitigate security risks to the extent reasonably practicable. Arista's security team works closely with each site to determine appropriate measures are in place to prevent unauthorized persons from gaining access to systems within which personal data is processed and continually monitor any changes to the physical infrastructure, business and known threats. They also monitor best practice measures used by others in the industry and carefully select approaches that meet both uniqueness in business practice and expectations of Arista. Arista balances its approach towards security by considering elements of control that include architecture, operations and systems.

2. **Physical Access controls:** Physical access controls/security measures at Arista's facilities/premises are designed to meet the following requirements:

    a) access to Arista's buildings, facilities and other physical premises shall be controlled and based upon business necessity, sensitivity of assets and the individual's role and relationship to Arista. Only personnel associated with Arista are provided access to Arista's facilities and physical resources in a manner consistent with their role and responsibilities in the organization;

    b) relevant Arista facilities are secured by an access control system. Access to such facilities is granted with an activated card only;

    c) all persons requiring access to facilities and/or resources are issued with appropriate and unique physical access credentials (e.g. a badge or key card assigned to one individual) by the IS function. Individuals issued with unique physical access credentials are instructed not to allow or enable other individuals to access the Arista's facilities or resources using their unique credentials (e.g. no "tailgating"). Temporary (up to 14 days) credentials may be issued to individuals who do not have active identities where this is necessary (i) for access to a specific facility and (ii) for valid business needs. Unique

credentials are non-transferable and if an individual cannot produce their credentials upon request they may be denied entry to Arista's facilities or escorted off the premises. At staffed entrances, individuals are required to present a valid photo identification or valid credentials to the security representative upon entering. Individuals who have lost or misplaced their credentials or other identification are required to enter through a staffed entrance and be issued a temporary badge by a security representative;

d) employees are regularly trained and reminded to always carry their credentials, store their laptops, portable devices and documents in a secure location (especially while traveling) and log out or shut down their computers when away from their desk;

e) visitors who require access to Arista's facilities must enter through a staffed and/or main facility entrance. Visitors must register their date and time of arrival, time of leaving the building and the name of the person they are visiting. Visitors must produce a current, government issued form of identification to validate their identity. To prevent access to, or disclosure of, company proprietary information visitors are not allowed unescorted access to restricted or controlled areas;

f) select Arista facilities use CCTV monitoring, security guards and other physical measures where appropriate and legally permitted;

g) locked shred bins are provided on most sites to enable secure destruction of confidential information/personal data;

h) for Arista's major data centers, security guards, UPS and generators, and change control standards are available;

i) for software development and infrastructure deployment projects, the IS function uses a risk evaluation process and a data classification program to manage risk arising from such activities.

Change Management

The IT organization manages changes to the corporate infrastructure, systems and applications through a centralized change management program, which may include testing, business impact analysis and management approval where appropriate. All relevant application and systems developments adhere to an approved change management process.

Security Incidents and Response Plan

1. **Security incident response plan:** Arista maintains a security incident response policy and related plan and procedures which address the measures that Arista will take in the event of loss of control, theft, unauthorized disclosure, unauthorized

access, or unauthorized acquisition of personal data. These measures may include incident analysis, containment, response, remediation, reporting and the return to normal operations.

2. **Response controls:** Controls are in place to protect against, and support the detection of, malicious use of assets and malicious software and to report potential incidents to the Arista's IS function or Service Desk for appropriate action. Controls may include, but are not limited to: information security policies and standards; restricted access; designated development and test environments; virus detection on servers, desktop and notebooks; virus email attachment scanning; system compliance scans; intrusion prevention monitoring and response; firewall rules; logging and alerting on key events; information handling procedures based on data type; e-commerce application and network security; and system and application vulnerability scanning. Additional controls may be implemented based on risk.

Data Transmission Control and Encryption

Arista shall, to the extent it has control over any electronic transmission or transfer of personal data, take all reasonable steps to ensure that such transmission or transfer cannot be read, copied, altered or removed without proper authority during its transmission or transfer. In particular, Arista shall:

1. implement industry-standard encryption practices in its transmission of personal data, including standard encryption practices from the National Institute of Standards and Technology (NIST). Industry-standard encryption methods used by Arista includes Transport Layer Security (TLS), a secure shell program such as SSH, and/or Internet Protocol Security (IPSec);

2. if technically feasible, encrypt all personal data, including, in particular any sensitive personal data or confidential information, when transmitting or transferring that data over any public network, or over any network not owned and maintained by Arista. The Arista's policy recognizes that encryption is ineffective unless the encryption key is inaccessible to unauthorized individuals and instructs personnel never to provide an encryption key via the same channel as the encrypted document;

3. for Internet-facing applications that may handle sensitive personal data and/or provide real-time integration with systems on a network that contains such information (including Arista's core network), a Web Application Firewall (WAF) may be used to provide an additional layer of input checking and attack mitigation. The WAF will be configured to mitigate potential vulnerabilities such as injection attacks, buffer overflows, cookie manipulation and other common attack methods.

System Access Controls

Access to Arista's systems is restricted to authorized users. Access is granted based on formal procedures designed to ensure appropriate approvals are granted so as to prevent access from unauthorized individuals. Such procedures include:

1. **admission controls** (i.e. measures to prevent unauthorized persons from using data processing systems):

    a) access is provided based on segregation of duties and least privileges in order to reduce the risk of misuse, intention or otherwise;

    b) access to IT systems will be granted only when a user is registered under a valid username and password;

    c) Arista has a password policy in place which requires strong passwords for user login to issued laptops, prohibits the sharing of passwords, prohibits the use of passwords that are also used for non-work functions, and advises users on what to do in the event their password or other login credentials are lost, stolen or compromised;

    d) mandatory password changes on a regular basis;

    e) automatic computer lock, renewed access to the PC only after new registration with a valid username and password;

    f) data and user classification determines the type of authentication that must be used by each system;

    g) remote access and wireless computing capabilities are restricted and require that both user and system safeguards are in place as well as user authentication.

2. **access controls** (i.e. measures to prevent unauthorized access to systems):

    a) access authorization is issued in respect of the specific area of work the individual is assigned to (i.e. work role);

    b) adjustment of access authorizations in case of changes to the working area, or in case an employee's employment is terminated for any reason;

    c) granting, removing and reviewing administrator privileges with the appropriate additional controls and only as needed to support the system(s) in question;

    d) event logs from key devices and systems are centrally collected and reported on an exceptions basis to enable incident response and forensic investigations.

Data Access Control

Arista applies the controls set out below regarding the access and use of personal data:

1. personnel are instructed to only use the minimum amount of personal data necessary in order to achieve Arista's relevant business purposes;

2. personnel are instructed not to read, copy, modify or remove personal data unless necessary in order to carry out their work duties;

3. third party use of personal data is governed through contractual terms and conditions between the third party and Arista which impose limits on the third party's use of personal data and restrict such use to what is necessary for the third party to provide services.

Separation Control

Where legally required, Arista will ensure that personal data collected for different purposes can be processed separately. Arista shall also ensure there is separation between test and production systems.

Job Control

Arista shall process personal data in accordance with the applicable services agreement between Arista and data exporter and in accordance with the instructions of the data exporter. The following controls will be implemented by the Arista:

1. personal data is processed only to the extent necessary for contractual performance;

2. personnel are subject to a written obligation of confidentiality;

3. diligent selection of (sub)processor and other service providers;

4. third party use of personal data is governed through contractual terms and conditions between the third party and Arista which impose limits on the third party's use of personal data and restricts such use to what is necessary for the third party to provide services;

5. clear instructions to (sub)processors on security measures for protecting privacy including the appropriate technical and organizational measures to safeguard the personal data to the same or higher level of protection as provided by Arista;

6. ongoing monitoring of (sub)processor's activities.

Availability Control

Arista protects personal data against accidental destruction or loss by following these controls:

1. personal data is retained in accordance with customer contract or, in its absence, Arista's record management policy and practices, as well as legal retention requirements;

2. hardcopy personal data is disposed of in a secure disposal bin or a crosscut shredder such that the information is no longer decipherable;

3. electronic personal data is given to Arista's IT Asset Management team for proper disposal;

4. appropriate technical measures are in place, including (without limitation): anti-virus software is installed on all systems; network protection is provided via firewall; network segmentation; user of content filter/proxies; interruption-free power supply; regular generation of back-ups; hard disk mirroring where required; fire safety system; water protection systems where appropriate; emergency plans; and air-conditioned server rooms.

Data Input Control

Arista has, where appropriate, measures designed to check whether and by whom personal data have been input into data processing systems, or whether such data has been modified or removed. Access to relevant applications is recorded.

System Development and Maintenance

Publicly released third party vulnerabilities are reviewed for applicability in the Arista environment. Based on risk to Arista's business and customers, there are predetermined timeframes for remediation. In addition, vulnerability scanning and assessments are performed on new and key applications and the infrastructure based on risk. Code reviews and scanners are used in the development environment prior to production to proactively detect coding vulnerabilities based on risk. These processes enable proactive identification of vulnerabilities as well as compliance.

Compliance

The information security, legal, privacy and compliance departments work to identify regional laws and regulations that may be applicable to Arista. These requirements cover areas such as, intellectual property of Arista and its customers, software licenses, protection of employee and customer personal information, data protection and data handling procedures, trans-border data transmission, financial and operational procedures, regulatory export controls around technology, and forensic requirements.

Mechanisms such as the information security program, the executive privacy council, internal and external audits/assessments, internal and external legal counsel consultation, internal controls assessment, internal penetration testing and vulnerability assessments, contract management, security awareness, security consulting, policy exception reviews and risk management combine to drive compliance with these requirements.

ANNEX C – APPROVED SUBCONTRACTORS

For a list of Subcontractors engaged by Arista, please visit:
https://www.arista.com/en/sub-processor.