INFINERA CORPORATION
VENDOR INFORMATION SECURITY REQUIREMENTS
Effective as of September 27, 2021

******(To the extent Vendor's policies and process regarding information security are already in place in a signed, written agreement with Infinera and such terms meet the minimum requirements outlined below, those terms shall apply to transactions with Infinera. Otherwise, the following terms are included in the contract terms for any products or services from Vendor.)**

Definitions.

(a) "**Affiliate**" of Party means an entity that, directly or indirectly, controls, is controlled by, or is under common control with that Party, where "control" means ownership or control of more than fifty percent (50%) of the voting power of securities or interests in the entity controlled.

(b) "**Aggregate**" means to combine or store Infinera Data with any data or information of Vendor or any third party.

(c) "**Anonymize**" means to use, collect, store, transmit or transform any data or information (including Infinera Data) in a manner or form that does not identify, permit identification of, and is not otherwise attributable to any user, device identifier, source, product, service, context, brand, or Infinera.

(d) "**Infinera Data**" means, individually and collectively: (a) all Infinera Confidential Information (as defined in the Agreement or in the non-disclosure agreement between the Parties); (b) all other data, records, files, content or information, in any form or format, acquired, accessed, collected, received, stored or maintained by Vendor or its Affiliates from or on behalf of Infinera or its Affiliates, or otherwise in connection with the Agreement, the services provided under the Agreement, or the Parties' performance of or exercise of rights under or in connection with the Agreement; and (c) derived from (a) or (b), even if Anonymized.

1. VENDOR INFORMATION SECURITY PROGRAM

Infinera Corporation and all of its Affiliates (collectively "**Infinera**") require all of its vendors, service providers and other business partners ("**You**" "**Your"** or "**Vendor**") to maintain a comprehensive written information security program ("**Vendor Information Security Program**") that includes technical, physical and organizational measures to ensure the confidentiality, security, integrity, and availability of Infinera Data provided by Infinera, and its employees, representatives, contractors, customers and Vendors and to protect against unauthorized access, use, disclosure, alteration or destruction of such Infinera Data. Infinera or You may be referred to herein as a "Party" or collectively as "Parties."

In particular, the Vendor Information Security Program shall include, but not be limited to, the following minimum requirements where appropriate or necessary to ensure the protection of Infinera Data. Additional terms may be applicable to Vendor, in the event Vendor provides cloud-based services:

- Access Controls – Policies, procedures, and physical and technical controls:

(i) to limit physical access to Your information systems and the facility or facilities in which they are housed to properly authorized persons;

(ii) to ensure that all members of Your workforce who require access to Infinera Data have appropriately controlled access, and to prevent those workforce members and others who should not have access from obtaining access;
(iii) to authenticate and permit access only to authorized individuals and to prevent members of Your workforce from providing Infinera Data or information relating thereto to unauthorized individuals; and
(iv) to encrypt and decrypt Infinera Data where required.

- Security Awareness and Training – A security awareness and training program for all members and levels of Your workforce (including management) on a regular basis, which includes training on how to implement and comply with Your Information Security Program.
- Security Incident Procedures – Policies and procedures to detect, respond to, and otherwise address security incidents, including procedures to monitor systems and to detect actual and attempted attacks on or intrusions into Infinera Data or information systems relating thereto, and procedures to identify and respond to suspected or known security incidents, mitigate harmful effects of security incidents, and document security incidents and their outcomes. If You become aware of any circumstance that may trigger either Party's obligations under applicable security breach laws, including any laws that require the notification of security breaches, You shall immediately provide written notice to Infinera via securityincident@Infinera.com and shall fully cooperate with Infinera to enable Infinera and You to carry out each Party's respective obligations under such security breach laws.
- Contingency Planning – Policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages Infinera Data or systems that contain Infinera Data, including a data backup plan and a disaster recovery plan and immediately providing a written notice to Infinera of such an incident, via securityincident@Infinera.com.
- Device and Media Controls – Policies and procedures regarding use of hardware and electronic media that contain Infinera Data and the movement of these items within and in and out of Your facilities, including policies and procedures to address the final disposition of Infinera Data, and/or the hardware or electronic media on which it is stored, and procedures for removal of Infinera Data from electronic media before the media are made available for re-use. You shall ensure that no Infinera Data is downloaded or otherwise stored on laptops or other portable devices unless they are subject to all of the protections required herein. Such protective measures shall include, but not be limited to, all devices accessing Infinera Data shall be encrypted and use up-to-date anti-malware detection prevention software.
- Audit controls – Implement hardware, software, services, platforms and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic information, including appropriate logs and reports concerning these security requirements and compliance therewith, in order to support an audit of such items and their use.
- Policies and Procedures – Policies and procedures to ensure the confidentiality, integrity, and availability of Infinera Data and protect it from accidental, unauthorized or improper disclosure, use, alteration or destruction.
- Storage and Transmission Security – Technical security measures to guard against unauthorized access to Infinera Data that is being transmitted over an electronic communications network, including a mechanism to encrypt Infinera Data in electronic form while in transit and in storage on networks or systems to which unauthorized individuals may have access.
- Assigned Security Responsibility – You shall designate a security official responsible for the development, implementation, and maintenance of your Information Security Program.
- Physical Storage Media – Policies and procedures to ensure that prior to any storage media containing Infinera Data being assigned, allocated or reallocated to another user, or prior to such storage media being permanently removed from a facility, you will securely delete in accordance with Section 2.3 (e.), such Infinera Data from both a physical and logical perspective or on any active network, such that the media contains no residual data, or if necessary physically destroy such storage media. You shall maintain an auditable program implementing the disposal and destruction requirements set forth in this Section for all storage media containing Infinera Data.

- Testing – You shall regularly test the key controls, systems and procedures of Your Information Security Program to ensure that they are properly implemented and effective in addressing the threats and risks identified. Tests should be conducted or reviewed by independent third parties or staff independent of those that develop or maintain such Information Security Program(s).
- Keep the Program Up-To-Date – You shall monitor, evaluate, maintain, and adjust, as appropriate, the Information Security Program in light of any relevant changes in technology or industry security standards, the sensitivity of the Infinera Data, internal or external threats to You or the Infinera Data, and Your own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to information systems.

2. INFINERA SECURITY POLICY

2.1. Infinera Security Policy ("Security Policy"). Vendor will comply in all respects with Infinera's information security requirements set forth in this Section 2. This Security Policy applies to Vendor's performance under any agreement, written, verbal, PO terms, etc. between Vendor and Infinera (the "**Agreement**") unless different or additional terms are already agreed to between the Parties in a separate written agreement and all access, collection, use, storage, transmission, disclosure, destruction or deletion of, and security incidents regarding Infinera Data. This Security Policy does not limit other obligations of Vendor, including under the Agreement or with respect to any laws that apply to Vendor, Vendor's performance under the Agreement, the Infinera Data or the Permitted Purpose (as defined below). To the extent this Security Policy directly conflicts with the Agreement, Vendor will promptly notify Infinera of the conflict and will comply with the requirement that is more restrictive and more protective of Infinera Data.

2.2. Permitted Purpose. Except as expressly authorized under the Agreement, Vendor may access, collect, use, store, and transmit only the Infinera Data expressly authorized under the Agreement and solely for the purpose of providing the goods and services under the Agreement, consistent with the licenses (if any) granted under the Agreement (the "**Permitted Purpose**"). Except as expressly authorized under the Agreement, Vendor will not access, collect, use, store or transmit any Infinera Data and will not Aggregate Infinera Data, even if Anonymized. Except with Infinera's prior express written consent, Vendor will not (A) transfer, rent, barter, trade, sell, rent, loan, lease or otherwise distribute or make available to any third party any Infinera Data or (B) Aggregate Infinera Data with any other information or data, even if Anonymized.

2.3. Basic Security Requirements. Vendor will, consistent with current best industry standards and such other requirements specified by Infinera based on the classification and sensitivity of Infinera Data, maintain physical, administrative and technical safeguards and other security measures (A) to maintain the security and confidentiality of Infinera Data accessed, collected, used, stored or transmitted by Vendor, and (B) to protect that information from known or reasonably anticipated threats or hazards to its security and integrity, accidental loss, alteration, disclosure and all other unlawful forms of processing. Without limitation, Vendor will comply with the following requirements:

(a) Firewall. Vendor will install and maintain a working network firewall to protect data accessible via the Internet and will keep all Infinera Data protected by the firewall at all times.

(b) Updates. 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 commercially reasonable security of the Infinera Data.

(c) Anti-malware. Vendor will at all times use anti-malware software and will keep the anti-malware software up to date. Vendor will mitigate threats from all viruses, spyware, and other malicious code that are or should reasonably have been detected.

(d) Encryption. Vendor will encrypt data at rest and data sent across open networks in accordance with industry best practices.

(e) Testing. Vendor will regularly test its security systems and processes to ensure they meet the requirements of this Security Policy.

(f) Access Controls. Vendor will secure Infinera Data, including by complying with the following requirements:

(i) Vendor will assign a unique ID to each person with computer access to Infinera Data.
(ii) Vendor will restrict access to Infinera Data to only those people with a "need-to-know" for a Permitted Purpose.
(iii) Vendor will regularly review the list of people and services with access to Infinera Data, and remove accounts (or advise Infinera to remove accounts) that no longer require access. This review must be performed at least once every 90 calendar days.
(iv) 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, Infinera Data and will require that all passwords and access credentials are kept confidential and not shared among personnel. Passwords must meet the following criteria: contain at least 12 characters; not match previous passwords, the user's login, or common name; must be changed whenever an account compromise is suspected or assumed; and are regularly replaced after no more than 90calendar days.
(v) Vendor will maintain and enforce "account lockout" by disabling accounts with access to Infinera Data when an account exceeds more than 10 consecutive incorrect password attempts.
(vi) Except where expressly authorized by Infinera in writing, Vendor will isolate Infinera Data at all times (including in storage, processing or transmission), from Vendor's and any third-party information.
(vii) If additional physical access controls are requested in writing by Infinera, Vendor will implement and use those secure physical access control measures.
(viii) Vendor will provide to Infinera on an annual basis or more frequently upon Infinera's written request, (1) log data about all use (both authorized and unauthorized) of Infinera's accounts or credentials provided to Vendor for use on behalf of Infinera (e.g., social medial account credentials), and (2) detailed log data about any impersonation of, or attempt to impersonate, Infinera personnel or Vendor personnel with access to Infinera Data.
(ix) Vendor will regularly review access logs for signs of malicious behavior or unauthorized access.
(x) Add requirement for Single Sign On ("SSO")

(g) Vendor Policy. Vendor will maintain and enforce information and network security policy terms for employees, subcontractors, agents, and its vendors that meets the standards set out in this Security Policy, including methods to detect and log policy violations. In the event Infinera reasonably suspects Infinera Data has been compromised, upon written request, Vendor will provide Infinera information about violations of Vendor's information and network security policy that could have given rise to the suspected incident involving Infinera Data, even if the event does not constitute a Security Incident.

(h) Subcontract. Vendor will not subcontract or delegate any of its material obligations under this Security Policy to any subcontractors without Infinera's prior written consent, such consent not to be unreasonably withheld. Notwithstanding the existence or terms of any subcontract or delegation, Vendor will remain responsible for the full performance of its obligations under this Security Policy and the performance of any subcontractors. The terms and conditions of this Security Policy will be binding upon Vendor's subcontractors and personnel. Vendor (a) will ensure that Vendor's subcontractors and personnel comply with this Security Policy, and (b) will be responsible for all acts, omissions, negligence and misconduct of its subcontractors and personnel, including (as applicable) violation of any applicable law, rule or regulation.

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

(j) Vendor personnel. Vendor will ensure that its personnel follows the applicable nondisclosure agreement terms between the Parties. Upon written request, Vendor will also (a) provide a list of Vendor personnel who have accessed or received the Infinera Data. Vendor will ensure that any personnel who no longer needs access to Infinera Data or who no longer qualifies as Vendor's personnel (leaves employment), will have access terminated within a reasonable time.

2.4. Access to Infinera Extranet and Vendor Portals. Infinera may grant Vendor access to Infinera Data via web portals or other non-public websites or extranet services on Infinera's or a third party's website or system (each, an "Extranet") for the Permitted Purpose. If Infinera permits Vendor to access any Infinera Data using an Extranet, Vendor must comply with the following additional requirements:

(a) Permitted Purpose. Vendor and its personnel will access the Extranet and access, collect, use, view, retrieve, download or store Infinera Data from the Extranet solely for the Permitted Purpose.

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

(c) Systems. 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 2.1(A) (Firewall); (ii) centralized patch management in compliance with Section 2.1(B) (Updates); (iii) operating system appropriate anti-malware software in accordance with Section 2.1(C) (Anti-malware); and (iv) for portable devices, full disk encryption.

(d) Restrictions. Except if approved in advance in writing by Infinera, Vendor will not download, mirror or permanently store any Infinera Data from any Extranet on any medium, including any machines, devices or servers.

(e) Account Termination. Vendor will terminate the account of each of Vendor's personnel and notify Infinera no later than 24 hours after any specific Vendor personnel who has been authorized to access any Extranet (a) no longer needs access to Infinera Data, (b) no longer qualifies as Vendor personnel (e.g., the personnel leaves Vendor's employment), or (c) no longer accesses Infinera information for 30 days or more.

(f) Third Party Systems.

(i) Vendor will give Infinera prior written notice and obtain Infinera's prior written approval before it uses any third-party system that stores or may otherwise have access to Infinera Data, unless (a) the data is encrypted in accordance with this Security Policy, and (b) the third-party system will not have access to the decryption key or unencrypted "plain text" versions of the data. Infinera reserves the right to require an Infinera security review (in accordance with Section 2.5 below) of the third-party system before giving approval.

(ii) If Vendor uses any third-party systems that store or otherwise may access unencrypted Infinera Data, Vendor must perform a reasonable security review of the third-party systems and their security controls. Upon written request, Vendor will provide Infinera periodic reporting about the third-party system's security controls in the format requested by Infinera (e.g., SAS 70, SSAE 16 or a successor report), or other recognized industry-standard report format if approved by Infinera to ensure compliance.

2.5. Data Retention and Destruction.

(a) Retention. Vendor will retain Infinera Data only for the purpose of, and as long as is necessary for, the Permitted Purpose or if Infinera requests Vendor delete the Infinera Data prior to completion of the Permitted Purpose, Vendor shall comply.

(b) Return or Deletion. Vendor will promptly (but within no more than 10 calendar days after Infinera's request) return to Infinera and permanently and securely delete all Infinera Data upon and in accordance with Infinera's notice requiring return and/or deletion. Also, Vendor will permanently and securely delete all live or active (online or network accessible) instances of the Infinera Data within 90 calendar days after the earlier of completion of the Permitted Purpose or termination or expiration of the Agreement, unless legally required to retain. If requested by Infinera, Vendor will certify in writing that all Infinera Data has been destroyed.

(c) Archival Copies. If Vendor is required by Law to retain archival copies of Infinera Data for tax or similar regulatory purposes, this archived Infinera Data must be stored in one of the following ways: as a "cold" or offline (i.e., not available for immediate or interactive use) backup stored in a physically secure facility; or 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.

(d) Recovery. 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 Infinera Data that is required to be deleted pursuant to the Agreement or this Security Policy will be re-deleted or overwritten from the recovered data in accordance within 24 hours after recovery occurs. If Vendor

performs a recovery for any purpose, no Infinera Data may be recovered to any third-party system or network without Infinera's prior written approval. Infinera reserves the right to require an Infinera security review of the third-party system or network before permitting recovery of any Infinera Data to any third-party system or network.

(e) Deletion Standards. All Infinera Data 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.Infinera), or a similar data protection structure or such other standards Infinera may require based on the classification and sensitivity of the Infinera Data being handled or disclosed to Vendor.

2.6. Forensic Destruction. Before disposing in any manner of any hardware, software, or any other media that contains Infinera Data, Vendor will perform a complete forensic destruction of the hardware, software or other media so that none of the Infinera Data can be recovered or retrieved in any form. Vendor will perform forensic destruction in accordance with the standards Infinera may require based on the classification and sensitivity of the Infinera Data. Vendor shall provide certificate of destruction upon request from Infinera.

(a) 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 Infinera Data that has not been forensically destroyed by Vendor.

2.7. Security Review.

(a) Risk Assessment Questionnaire. Infinera requires all Vendors to undergo a Vendor Risk Assessment, to be triggered by providing updated responses to Infinera's risk assessment questionnaire provided to Vendor. Infinera may ask for this information periodically depending on the assessed risk of the Vendor, but at lease once per year Infinera will seek such information. To the extent Infinera does not perform a Vendor Risk Assessment on an annual basis, Infinera is not prejudiced from seeking information or performing an assessment in subsequent years.

(b) Certification. Upon Infinera's written request, Vendor will certify in writing to Infinera that it is in compliance with this Infinera Security Policy.

(c) Other Reviews. Infinera reserves the right to periodically review the security of systems that Vendor uses to process Infinera Data, upon written prior notice to Vendor. Vendor will reasonably cooperate and provide Infinera with all required information within a reasonable time frame, but no more than 30 calendar days from the date of Infinera's request, unless the Parties agree otherwise.

(d) Remediation. If any security review identifies any noted deficiencies, Vendor will, at its sole cost and expense, take all actions necessary to address those deficiencies within an agreed upon, reasonable timeframe.

2.8. Security Breach.

(a) Vendor will inform Infinera via securityincident@infinera.com without undue delay (buy not longer than 24 hours from Vendor's reasonable knowledge of a security breach as defined by applicable law(s) (i) containing Infinera Data, or (ii) managed by Vendor with controls substantially similar to those protecting Infinera Data (each, a "Security

Incident"). Vendor will remedy each Security Incident in a timely manner and provide Infinera written details regarding Vendor's internal investigation regarding each Security Incident. Vendor agrees not to notify any regulatory authority, nor any customer, on behalf of Infinera unless Infinera specifically requests in writing that Vendor do so and Infinera reserves the right to review and approve the form and content of any notification before it is provided to any such third party. Vendor will reasonably cooperate and work together with Infinera to formulate and execute a plan to rectify all confirmed Security Incidents.

(b) Vendor will inform Infinera without undue delay (no longer than 3 business days) when Infinera Data is being sought in response to legal process, subpoena, or by applicable law.