Infinera Corporation and all of its Affiliates (collectively "Infinera") require all of its vendors, service providers and other business partners, including Affiliates ("You" and/or "Your") to maintain a comprehensive written information security program ("Vendor Information Security Program") that aligns to the latest versions of ISO/IEC 27001 and ISO/IEC 27002 which 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. **Affiliate** of a 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. 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. **Infinera Data** means, individually and collectively: (a) all Infinera non-public 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 You 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. Additional terms may be applicable to Vendor, in the event Vendor provides cloud-based services:

1. VENDOR INFORMATION SECURITY PROGRAM

1.1. Basic Security Requirements – Policies, procedures, and physical and technical controls shall meet the following minimum requirements:

1.1.1. You will limit physical access to Your information systems and the facility or facilities in which they are housed to properly authorized persons;

1.1.2. You will ensure that all vendor personnel including employees, contractors, and subcontractors, 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.

1.1.3. You 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.

1.1.4. You will keep your 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 Infinera Data.

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

1.1.6. You will encrypt data at rest and in transit in accordance with industry best practices.

1.1.7. You will assign a unique ID to each person with computer access to Infinera Data.

1.1.8. You will restrict access to Infinera Data to only those people with a "need to know" for a permitted purpose.

1.1.9. You 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.

1.1.10. You will not use manufacturer-supplied defaults for system passwords and other security parameters on any operating systems, software or other systems. You will mandate and ensure the use of system-enforced "strong passwords" in accordance with the standards in this Section 1.1.10 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 90 calendar days.

1.1.11. You 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.

1.1.12. Access to Infinera Data shall be controlled through an authentication process that includes multi-factor authentication.

1.1.13. Except where expressly authorized by Infinera in writing, You will isolate Infinera Data at all times (including in storage, processing or transmission), from Your and any third-party information.

1.1.14. If additional physical access controls are requested in writing by Infinera, You will implement and use those secure physical access control measures.

1.1.15. You 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 You 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 Your personnel with access to Infinera Data.

1.1.16. You will regularly review access logs for signs of malicious behavior or unauthorized access.

1.1.17. Conflicting duties and areas of responsibility should be segregated.

1.2. 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.

1.3. 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.

1.4. 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.

1.5. 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.

1.6. Assigned Security Responsibility – You shall designate a security official responsible for the development, implementation, and maintenance of your Information Security Program. Roles and responsibilities-users and stakeholders should be identified and assigned, informed of their responsibilities and trained in all aspects of their roles. Management shall be accountable for the actions or inactions of their staff and suppliers.

1.7. Physical Storage Media Assigned to Subsequent User – 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 , 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.

1.8. 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. Tests should be conducted or reviewed by independent third parties or staff independent of those that develop or maintain such Information Security Program(s).

1.9. 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.

1.10. Threat intelligence - You shall utilize threat intelligence to ensure security threats are identified and the appropriate actions are taken to mitigate any perceived threats.

1.11. Asset Management – You shall maintain a strong asset inventory and shall maintain such assets in accordance with industry best practices and manufacturer recommendations. Your asset management program shall ensure the appropriate issuance, change, and return of assets, including information as an asset.

1.12. Data Classification and Labeling - You shall maintain and practically use a data classification and labeling program.

1.13. Supplier Relationships -You shall ensure that all downstream and upstream vendors have a complete set of controls in place that are commensurate with the types of data and risk to such data. Any sharing of Infinera non-public data shall be approved by Infinera. when managing supplier relationships, You shall ensure that all third-party relationships that affect Infinera are monitored,

protected by the appropriate legal instruments (contracts), and that Service-Level Agreements meet or exceed the requirements the vendor has with Infinera. Third party agreements shall include all aspect of security management, where appropriate and incident response shall include notifying Infinera of any security incidents that affect or could affect the Confidentiality, Integrity, or Availability of Infinera data. You shall have an independent review of their program on an annual basis and shall provide Infinera with a summary of the results. In the event that a high or critical finding or any finding that could reasonably place Infinera data or systems in danger of a breach, You shall immediately contact Infinera and discuss the mitigation strategy. Should Infinera determine that the vulnerability is too risky for Infinera, Infinera may, at our discretion, opt to remove all data from You site and pause or cancel the contract until the vulnerability is corrected with no penalties.

1.14. **Legal Requirements** - You are accountable for ensuring compliance with ALL laws, regulations, and any binding requirements that are applicable to Infinera as they relate to cybersecurity and Privacy.

1.15. **Right to audit** - Infinera or our designated representative shall be allowed to audit You for any concerns to any law, regulation, or any binding requirements that Infinera must follow. This includes any concerns about the ability of You to meet Your security requirements. Audits shall be scheduled in advance by both parties. Infinera shall incur all internal costs associated with the audit but shall not be accountable for any vendor time or costs involved in these audits. You will 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.

1.16. **Risk assessment** - You shall maintain a risk management program that addresses and detects areas of risk. Program shall be cyclic and require assessment upon any material change. This program shall ensure constant improvement of the program.

2. INFINERA SECURITY POLICY

2.1. Infinera Security Policy ("Security Policy"). You will comply in all respects with Infinera's information security requirements set forth in this Section 2. This Security Policy applies to Your performance under any agreement, written, verbal, PO (Purchase Order) terms, etc. between You 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 You, including under the Agreement or with respect to any laws that apply to You, Your 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, You 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, You 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, You will not access, collect, use, store or transmit any Infinera Data and will not Aggregate

Infinera Data, even if Anonymized. **Aggregate** means to combine or store Infinera Data with any data or information of You or any third party. **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. Except with Infinera's prior express written consent, You will not (A) transfer, 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. Use and Transfer Limitations. You must not access, collect, store, retain, transfer, use or otherwise process in any manner any Infinera Data, except: (a) in the interest and on behalf of Infinera; (b) as directed by authorized personnel of Infinera in writing; and (c) in accordance with applicable law. Without limiting the generality of the foregoing, You may not make Infinera Data accessible to any subcontractors or relocate Infinera Data to new locations, except as set forth in written agreements with, or written instructions from Infinera. You must return or delete any Infinera Data at the end of Your relationship with Infinera and, at any time, at Infinera's request. You must impose contractual obligations on all employees, contractors and onward recipients of Infinera Data that are at least as protective of Infinera Data as these Requirements.

2.4. Cooperate with Compliance Obligations. At Infinera's reasonable request, You must: (a) execute a business associate agreement under the U.S. Health Insurance Portability and Accountability Act of 1996 and related regulations, as amended ("HIPAA") as well as similar agreements as required under other jurisdictions' laws, (b) contractually agree to comply with laws and industry standards designed to protect Infinera Data, including, without limitation, the Standard Contractual Clauses approved by the European Commission for data transfers to processors, PCI Standards, as well as similar and other frameworks, if and to the extent such frameworks apply to any Infinera Data that You come into contact with; or (c) allow Infinera to terminate certain or all contracts with You in the event of material non-compliance with (a) or (b) above, subject to (i) a proportionate refund of any prepaid fees, (ii) transition or migration assistance, at Your expense, as reasonably required by Infinera, and (iii) without applying any early termination charges or other extra charges.

2.5. No Information Selling or Sharing for Advertising. You acknowledge and confirm that You do not receive any Infinera Data as consideration for any services or other items that You provide to Infinera. You shall not have, derive or exercise any rights or benefits regarding Infinera Data. You must not sell or share any Infinera Data, as the terms "sell" and "share" are defined in the California Consumer Privacy Act of 2018, as amended, including by the California Privacy Rights Act of 2020 ("CCPA") or under any other laws. You must not collect, retain, use, or disclose any Infinera Data (a) for targeted or cross-context behavioral advertising, (b) but for the business purposes specified in a written contract with Infinera, or (c) outside the direct business relationship with Infinera. You must not combine Infinera Data with other data if and to the extent this would be inconsistent with limitations on service providers under the CCPA or other laws. You certify that You understand the rules, requirements and definitions of the CCPA, and all restrictions in the Data Protection Standards. You agree to refrain from taking any action that would cause any transfers of Infinera Data to or from You to qualify under the CCPA or other laws as "sharing" for advertising purposes or as "selling" personal information

2.6. Subcontract. You 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, You 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 Your subcontractors and personnel. You (a) will ensure that Your 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.

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

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

2.9. Access to Infinera Extranet and Vendor Portals. Infinera may grant You 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 You to access any Infinera Data using an Extranet, You must comply with the following additional requirements:

2.9.1. Permitted Purpose. You 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.

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

2.9.3. Systems. You will access the Extranet only through computing or processing systems or applications running operating systems managed by You and that include the minimum requirements set forth in Section 1.1 of these Requirements.

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

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

2.9.6. Third Party Systems.

2.9.6.1. (i) You 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 of the third-party system before giving approval.

2.9.6.2. (ii) If You uses any third-party systems that store or otherwise may access unencrypted Infinera Data, You must perform a reasonable security review of the third-party systems and their security controls. Upon written request, You 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.

2.10. Data Retention and Destruction.

2.10.1. Retention. You will retain Infinera Data only for the purpose of, and as long as is necessary for, the Permitted Purpose. Upon Infinera's request, You will delete the Infinera Data prior to completion of the Permitted Purpose.

2.10.2. Return or Deletion. You 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, You 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, You will certify in writing that all Infinera Data has been destroyed.

2.10.3. Archival Copies. If You are 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.

2.10.4. Recovery. If You perform a "recovery" (i.e., reverting to a backup) for the purpose of disaster recovery, You will have and maintain a process that ensures that all Infinera Data that is required to be deleted pursuant to an Agreement or these Requirements will be re-deleted or overwritten from the recovered data in accordance within 24 hours after recovery occurs. If You perform 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.

2.10.5. Deletion Standards. All Infinera Data deleted by You will be deleted in accordance with the NIST Special Publication 800-88 Revision 1, Guidelines for Media Sanitation December 18, 2014 (available at NIST Special Publication 800-88, Revision 1: Guidelines for Media Sanitization | NIST), 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 You.

2.11. Forensic Destruction. Before disposing in any manner of any hardware, software, or any other media that contains Infinera Data, You 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. You will perform forensic destruction in accordance with the standards Infinera may require based on the classification and sensitivity of the Infinera Data. You shall provide certificate of destruction upon request from Infinera.

2.11.1. You 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 Your business, or any other disposition) any hardware, software or other media that contains Infinera Data that has not been forensically destroyed by You. You further acknowledge and confirm that You do not receive any Infinera Data as consideration for any services or other items that You provide to Infinera.

2.12. Security Review.

2.12.1. 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 You. Infinera may ask for this information periodically depending on the assessed risk of the vendor, but at least 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.

2.12.2. Certification. Upon Infinera's written request, You will certify in writing to Infinera that You are in compliance with this Infinera Security Policy.

2.12.3. 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 You. You 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.

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

2.13. Security Breach.

2.13.1. If You become aware of unauthorized access or potential security breach related to Infinera Data or systems, You must immediately notify Infinera (and not longer than 24 hours) at securityincident@infinera.com, consult and cooperate with investigations and potentially required notices, and provide any information reasonably requested by Infinera. You must also indemnify Infinera from any resulting damages and costs, including, without limitation, remediation of the incident, identity protection assistance and services procured for, data subjects and reasonable attorneys and technical consultant fees for Infinera's handling of the incident.

2.13.2. You 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.

2.14. EEA Personal Data: With respect to any Infinera Data that is subject to the GDPR or similar laws of other countries as "personal data," You accept the GDPR Standard Contractual Clauses 2021 promulgated by Commission implementing decision (EU) 2021/914 of 4 June 2021, Modules 1 to 3, and you will provide completed Annexes, a list of subprocessors and a transfer impact assessment (as required by Clause 14) without undue delay.