



CISCO

Cisco Systems Inc.

General Terms & Appendices

In this document

- General Terms
- Cisco RMA Policy for Warranty and Hardware Support Contract Returns
- Customer Content: data brief
- Personal Data: data brief
- Systems Information data brief
- Data Protection Agreement
- Information Security Exhibit
- Software License Portability Policy
- Software License Transfer and Re-Use Policy



Website references

Throughout the Cisco terms, references to external websites will instead point to attachments included in this package. Links and webpage references in the left column shall mean the document (and section) in the right column.

Link / Reference	Document / Section
Warranties Product Warranties https://www.cisco.com/go/warranty	General Terms & Appendices, Warranty <i>section</i>
Cisco General Terms webpage Software General Terms	General Terms & Appendices,
Data Protection Agreement	General Terms & Appendices, Data Protection Agreement <i>section</i>
Information Security Exhibit	General Terms & Appendices, Information Security Exhibit <i>section</i>
Customer Content – Data Brief webpage	General Terms & Appendices, Customer Content: Data Brief <i>section</i>
Personal Data – Data Brief	General Terms & Appendices, Personal Data: Data Brief <i>section</i>
Systems Information – Data Brief	General Terms & Appendices, Systems Information: Data Brief <i>section</i>
Cisco Software Transfer and Re-licensing Policy http://network.cisco.com/en/US/prod/cisco_software_transfer_relicensing_policy.html .	General Terms & Appendices, Software Transfer and Re-licensing Policy <i>section</i>
Software Portability Policy Software License Portability Policy https://www.cisco.com/go/softwareterms https://network.cisco.com/c/en/us/products/end-user-license-agreement.html	General Terms & Appendices, Software License Portability Policy <i>section</i>
Cisco RMA Policy for Warrant and Hardware Support Contract Returns	General Terms & Appendices, RMA <i>section</i>
Link / Reference	Website
Offer Descriptions Product Specific Terms Product Descriptions Product Offer Descriptions	Follow to website via URL in document
Offer Descriptions Service Specific Terms Service Descriptions Service Offer Descriptions Software Support Service Solution Support	Follow to website via URL in document

General Terms

1. Scope and applicability

- 1.1 These terms (the “**General Terms**”) govern Your access to, and use of, Cisco Offers and incorporate any Supplemental Terms and Offer Descriptions available at <https://www.cisco.com/c/en/us/about/legal/cloud-and-software/software-terms.html> applicable to Your Order. Capitalized terms are defined in section 14 (Definitions).
- 1.2 You agree to these terms by finalizing and executing Your written Order or through Your express written agreement, whichever happens first. These terms apply independently of any contract You may have with a Cisco Partner.

2. Use Rights

- 2.1 **License and right to use.** Cisco grants You, for Your direct benefit, a non-exclusive:
 - (a) license to use Software and Cisco Content; and
 - (b) right to use Subscription Offers, including Cloud Services,in accordance with Your Order or as otherwise agreed in writing (collectively, the “**Use Rights**”). Your Use Rights are non-transferable (except Software as permitted under the Transfer Policies).
- 2.2 **Limits on usage.** You may not:
 - (a) transfer, sell, sublicense, monetize or provide the functionality of any Cisco Offer to any third party, except as authorized by Cisco;
 - (b) use the Software on second hand or refurbished Cisco devices or use Software licensed for a specific device on a different device unless authorized by Cisco or permitted under the Transfer Policies;
 - (c) remove, change, or conceal any product identification, copyright, proprietary, intellectual property notices or other marks from any Cisco Offer;
 - (d) reverse engineer, decompile, decrypt, disassemble, modify, or make derivative works of Cisco Offers; or (e) use Cisco Content other than as reasonably needed to exercise Your Use Rights.
- 2.3 **Acceptable use.** You will ensure Your access or use of Software or Subscription Offers does not:
 - (a) violate applicable laws or the rights of any third party; or
 - (b) impede or interfere with the security, stability, availability or performance of any Cloud Service, or any other network or service (e.g., denial-of-service attacks, penetration testing or distribution of malware).
- 2.4 **Suspension.** Cisco may temporarily suspend Your access to Software or Subscription Offers if it reasonably believes that You or an Authorized User have materially breached section 2.3(b) (Acceptable use).
- 2.5 **Use by third parties.** If You permit Authorized Users to access Cisco Offers on Your behalf:
 - (a) You will make sure all Authorized Users follow these terms; and
 - (b) You are liable for any breach of these terms by an Authorized User.
- 2.6 **Interoperability requirements.** If required by law, Cisco will promptly provide the information You request to achieve interoperability between applicable Cisco Offers and another independently created program on terms that reasonably protect Cisco’s proprietary interests.
- 2.7 **Use with third party products.** Cisco does not support or guarantee integration with third party technologies or services unless they are included as part of a Cisco Offer or agreed in writing.
- 2.8 **Changes to Subscription Offers.** Cisco may change its Subscription Offers, typically to enhance them or add features. These changes will not materially reduce the core functionality of the affected Subscription Offers during the Use Term.

planned maintenance when reasonably possible. If Cisco performs emergency maintenance without notice, it will take reasonable steps to reduce any disruption of affected Subscription Offers.

- 2.10 **Open-source technology.** Separate license terms apply to third party open-source technology used in Cisco Offers. Open-source terms are found at [Cisco's Open Source](#) webpage. As long as You use Cisco Offers according to these General Terms, Cisco's use of open-source technology in Cisco Offers will not impede Your exercise of Use Rights or cause Your software to become subject to an open-source license.

3. Free trials

- 3.1 **Accessing Free Trials.** Your Approved Source may let You access or use Cisco Offers on a trial, evaluation, beta or other free-of-charge basis ("**Free Trial**"). You may only access or use the Free Trial for the period specified ("**Free Trial Period**") and under any additional terms specified by Your Approved Source in writing. If no Free Trial Period is specified, You may only access or use the Free Trial for 60 days after the Free Trial is available to You. Free Trials may not come with support and may be incomplete or have errors. Unless agreed in writing by Cisco, You will not use the Free Trial in a production environment.
- 3.2 **Ending Free Trials.** At the end of a Free Trial, You will promptly Return the Cisco Offers as described in the Free Trial terms. Your Approved Source may change or terminate a Free Trial at its discretion with reasonable notice.
- 3.3 **Continued use and disclaimer.**
- (a) If You continue accessing a Cisco Offer after a Free Trial Period or fail to Return a Cisco Offer, You will pay any applicable fees reasonably charged by Your Approved Source.
 - (b) **Unless agreed by Cisco in writing or required by law, Free Trials are provided "AS-IS" without any express or implied warranties.**

4. End of life

- 4.1 **Notification.** Cisco may end the life of Cisco Offers by providing notice at the [End-of-Sale and End-of-Life Products](#) webpage.
- 4.2 **Pre-paid Cloud Service.** If Your Approved Source is prepaid a fee for Your use of a Cloud Service that is end of life before Your then-current Use Term ends, Cisco will either (a) provide You with a generally available alternative offer, or (b) if Cisco cannot reasonably provide an alternative offer, it will credit the unused balance of fees paid for the relevant Cloud Service to Your Approved Source or You (if Cisco is the Approved Source) once You Return the Cloud Service.
- 4.3 **Credit.** Credits issued under section 4.2 (Pre-paid Cloud Service) are calculated from the last date the applicable Cloud Service is available to the end of the applicable Use Term and may be applied only towards the future purchase of Cisco Offers.

5. Paying Your Approved Source

You will pay Your Approved Source all amounts due under Your Orders, including fees for additional consumption of a Subscription Offer or under a Buying Program.

6. Confidentiality

- 6.1 **General obligation.** A recipient of Confidential Information will protect that Confidential Information using the same standard of care it uses to protect its own confidential information of a similar nature, but no less than a reasonable standard of care. This section 6 (Confidentiality) will not apply to information which:
- (a) is known by the recipient without confidentiality obligations;
 - (b) is or has become public knowledge through no fault of the recipient; or (c) is independently developed by, or for, the recipient.
- 6.2 **Permitted recipients.** A recipient of Confidential Information will not disclose Confidential Information to any third party, except to its employees, Affiliates and contractors who need to know. The recipient is liable for a breach of this section 6 by its permitted recipients and must ensure each of those permitted recipients have written confidentiality obligations at least as restrictive as the recipient's obligations under these terms.
- 6.3 **Required disclosures.** The recipient may reveal Confidential Information if required by law (including under a court order) but only after it notifies the discloser in writing (if legally permissible). A recipient will reasonably cooperate with a discloser's reasonably requested protective actions, at the discloser's expense. Cisco recognizes that Federal agencies are subject to the Freedom of Information Act, 5 U.S.C. 552, which may require that certain information be released, despite being characterized as "confidential" by the vendor.

course of business. Retained Confidential Information will continue to be subject to this section 6 for five years, or until the Confidential Information is no longer a trade secret under applicable law.

7. Privacy and security

- 7.1 Cisco respects Your Data and will access and use Data in accordance with the Data Briefs.
- 7.2 In addition, if Cisco processes Personal Data or Customer Content, Cisco will process such data according to:
 - (a) the Data Processing Terms for Personal Data (which are attached hereto and incorporated by reference);
 - (b) the security measures described in Cisco’s Information Security Exhibit;
 - (c) the Privacy Data Sheets applicable to the relevant Cisco Offer; and
 - (d) privacy and data protection laws applicable to Cisco Offers.
- 7.3 You will ensure Your use of Cisco Offers (including collection, processing and use of Customer Content with Cisco Offers) complies with privacy and data protection laws applicable to Your Cisco Offers, including industry-specific requirements. You are also responsible for providing notice to, and getting consents from individuals whose data may be collected, processed, transferred and stored through Your use of Cisco Offers.

8. Ownership of intellectual property

- 8.1 Unless agreed in writing, nothing in these terms transfers ownership in any intellectual property rights. You keep ownership of Customer Content and Cisco keeps ownership of Cisco Offers and Cisco Content.
- 8.2 Cisco may use any feedback You provide in connection with Your use of Cisco Offers.

9. Intellectual property indemnity

- 9.1 **Claims.** Cisco will have the right to intervene to defend any third-party claim against You asserting that Your valid use of a Cisco Offer infringes a third party’s patent, copyright or registered trademark (the “**IP Claim**”). Cisco will indemnify You against the final judgment entered by a court of competent jurisdiction or any settlements arising out of an IP Claim, if You:
 - (a) promptly notify Cisco in writing of the IP Claim (but failure to promptly notify Cisco only limits Cisco’s obligations to the extent it is prejudiced by the delay);
 - (b) fully cooperate with Cisco in the defense of the IP Claim; and
 - (c) grant Cisco the right to exclusively control the defense and settlement of the IP Claim, and any appeal.Cisco does not have to reimburse You for attorney fees and costs incurred before Cisco receives notification of the IP Claim. You may retain Your own legal representation at Your own expense. Nothing contained herein shall be construed in derogation of the U.S. Department of Justice’s right to defend any claim or action brought against the U.S., pursuant to its jurisdictional statute 28 U.S.C. §516.
- 9.2 **Additional remedies.** If an IP Claim prevents or is likely to prevent You from accessing or using the applicable Cisco Offer, Cisco will either get the right for You to continue using the Cisco Offer or replace or modify the applicable Cisco Offer with non-infringing functionality that is at least equivalent. If Cisco determines those options are not reasonably available, then Cisco will provide a prorated refund for the impacted Cisco Offer.
- 9.3 **Exclusions.** Cisco has no duty regarding any IP Claim to the extent based on:
 - (a) any designs, specifications or requirements provided by You, or on Your behalf;
 - (b) modification of a Cisco Offer by You, or on Your behalf;
 - (c) the amount or duration of use made of a Cisco Offer, revenue You earned, or services You offered;
 - (d) combination, operation, or use of the Cisco Offer with non-Cisco products, software, content or business processes; or
 - (e) Your failure to change or replace the Cisco Offer as required by Cisco.
- 9.4 To the extent allowed by law, this section 9 states Your only remedy regarding an IP Claim against You.

10. Performance standards

- 10.1 **Service Level Agreement.** Cisco Offers will comply with applicable Service Level Agreements, as set out in the corresponding Offer Description.
- 10.2 **Warranties.** Cisco provides these warranties for Cisco Offers:

Warranty	Cisco Offer		
	Hardware	Software	Subscription Offers

Cisco warrants that the Cisco Offer substantially complies with the Documentation as follows:

(a) if the Cisco Offer is a Subscription Offer, starting from commencement of the service, for the duration of the services; and

(b) if the Cisco Offer is Hardware or Software, for 90 days from shipment or longer as stated in Documentation, or as set out in [Product Warranties](#) webpage.



Cisco warrants it will use commercially reasonable efforts and methods to deliver the Cisco Offer free from Malicious Code.



Cisco warrants that the Cisco Offer is free from defects in material and workmanship for 90 days from shipment or longer as stated in Documentation or as set out in [Product Warranties](#) webpage.



To make a claim for breach of these warranties, promptly notify both Cisco and Cisco Partner (if they are Your Approved Source) within any specified warranty period.

10.3 **Qualifications**

- (a) You may have legal rights in Your country that prohibit or restrict the limitations set out in this section 10. This section 10 applies only to the extent permitted under applicable law.

- (b) Section 10.2 does not apply if Your breach of the General Terms contributes to the breach of warranty, or if the Cisco Offer:
 - (1) has not been used according to its Documentation;
 - (2) has been altered, except by Cisco or its authorized representative;
 - (3) has been subjected to abnormal or improper environmental conditions, accident or negligence, or installation or use inconsistent with Cisco's instructions or the terms on which it is supplied by Cisco;
 - (4) is provided under a Free Trial; or
 - (5) has not been provided by an Approved Source.
- (c) Your sole remedy for breach of a warranty under section 10.2 is, at Cisco's option, either: (1) repair or replacement of the applicable Cisco Offer; or
 - (2) a refund of either:
 - (A) the fees paid for Use Rights in the non-conforming Software;
 - (B) the fees paid for the period in which the Subscription Offer did not conform less any amounts paid or owed under a Service Level Agreement; or (C) the fees paid for the non-conforming Hardware.
- (d) **Except as provided in Section 10.2 above, and to the extent allowed by law, Cisco makes no express or implied warranties of any kind regarding the Cisco Offers. This disclaimer includes any warranty, condition or other term as to merchantability, merchantable quality, fitness for purpose or use, course of dealing, usage of trade, or non-infringement. Cisco does not warrant that Cisco Offers will be secure, uninterrupted or error-free.**

11. Liability

- 11.1 **Excluded liability.** Neither party is liable for:
 - (a) indirect, incidental, reliance, consequential, special or exemplary damages; or
 - (b) loss of actual or anticipated revenue, profit, business, savings, data, goodwill or use, business interruption, damaged data, wasted expenditure or delay in delivery (in all cases, whether direct or indirect).
- 11.2 **Liability cap.** Each party's entire liability for all claims relating to these terms will not exceed the greater of: (a) the fees paid to Cisco for the specific Cisco Offer that is the subject of the claim in the 12 months before the first incident giving rise to such liability; or (b) \$100,000 USD. This cap is cumulative for all claims (not per incident) and applies collectively to each party and its Affiliates (not per Affiliate).
- 11.3 **Unlimited liability.** Nothing in this section 11 limits or excludes liabilities that cannot be excluded or limited under applicable law, or for:
 - (a) bodily injury or death resulting directly from the other party's negligence;
 - (b) fraudulent misrepresentation or wilful misconduct;
 - (c) breach of confidentiality obligations, unless the breach relates to section 7 (Privacy and security); (d) failure to pay for Cisco Offers;
 - (e) misuse or misappropriation by a party of the other party's intellectual property rights; or (f) failure to comply with export control obligations.

12. Termination

- 12.1 **Material breach.** When the End User is an instrumentality of the U.S., recourse against the United States for any alleged breach of this Agreement must be brought as a dispute under the contract Disputes Clause (Contract Disputes Act). During any dispute under the Disputes Clause, for so long as Your Order subject to the dispute has not expired, Cisco shall proceed diligently with performance of this Agreement, pending final resolution of any request for relief, claim, appeal, or action arising under the Agreement, and comply with any decision of the Contracting Officer. There is no ongoing obligation for Cisco to continue to provide any Offer after the expiration of the term in the Order.
- 12.2 **Reserved.** .
- 12.3 **Effect of termination or expiration.** You will Return applicable Cisco Offers (except any Cisco Offer in which title has transferred to You) at the end of Your Use Term or upon termination of an Order.

13. General provisions

- 13.1 **Survival.** Sections 5 (Paying Your Approved Source), 6 (Confidentiality), 7 (Privacy and security), 8 (Ownership of intellectual property), 9 (IP Indemnity), 10 (Performance standards), 11 (Liability), 12 (Termination) and 13 (General provisions) survive termination of these terms.
- 13.2 **No agency.** These terms do not create any agency, partnership, joint venture, or franchise relationship.
- 13.3 **Assignment and subcontracting.**
- (a) Except as set out below, neither party may assign or novate these terms in whole or in part without the other party's written consent which will not be unreasonably withheld. Cisco may assign these terms in connection with the sale of a part of its business, or to its Affiliates in accordance with the provisions set forth at FAR 42.1204.
 - (b) Cisco may subcontract any performance associated with any Cisco Offer to third parties if such subcontract is consistent with these terms and does not relieve Cisco of any of its obligations under these terms.
- 13.4 **Third party beneficiaries.** These terms do not grant any right or cause of action to any third party.
- 13.5 **Use records.** You will keep reasonable records of your use of the Cisco Offers. You will let Cisco and its auditors who are under a written obligation of confidentiality access records of Your use of the Cisco Offers (including books, systems, and accounts) within 30 days' notice from Cisco. Cisco may not give this notice more than once in any 12-month period and will conduct any audit during Your normal business hours subject to Government security requirements. If the verification process reveals underpayment of fees, You will pay these fees within 30 days.
- 13.6 **Changes to these terms.** The version of the General Terms applicable to Your Order is the version published at the [Cisco General Terms](#) webpage when the Order is placed. If Cisco changes these terms or any of its parts, these changes will be published at the [Cisco General Terms](#) webpage. These non-material changes will only apply to Cisco Offers Ordered or renewed after the date of the change.
- 13.7 **Compliance with laws**
- (a) **General.** Cisco will comply with all applicable laws relating to providing Cisco Offers under these terms. You will comply with all applicable laws relating to Your receipt and use of Cisco Offers, including sectorspecific requirements and obtaining required licenses or permits (if any).
 - (b) **Trade Compliance.** Cisco Offers are subject to US and other export control and sanctions laws around the world. These laws govern the use, transfer, export and re-export of Cisco Offers. Each party will comply with such laws and obtain all licenses or authorizations it is required to maintain. Please refer to Cisco's trade compliance policies at the [General Export Compliance](#) webpage.
- 13.8 **Governing law and venue.** These terms, and any disputes arising from them, are subject to the governing law and exclusive jurisdiction and venue listed below, based on Your primary place of business. Each party consents and submits to the exclusive jurisdiction of the courts in the listed venue. These laws apply despite conflicts of laws rules or the United Nations Convention on Contracts for the International Sale of Goods. Despite the below, either party may seek interim injunctive relief in any court of appropriate jurisdiction regarding any alleged breach of confidentiality obligations or intellectual property or proprietary rights.

Your Primary Place of Business	Governing Law	Jurisdiction and Venue
United States, Latin America or the Caribbean, or a location not specified below	State of California, United States	Superior Court of California, County of Santa Clara and Federal Courts of the Northern District of California
Africa, Asia*, Europe*, Middle East, Oceania*	England	English Courts
Australia	State of New South Wales, Australia	State and Federal Courts in New South Wales
Canada	Province of Ontario, Canada	Courts of the Province of Ontario
Mainland China	People's Republic of China	Hong Kong International Arbitration Center
Italy	Italy	Court of Milan
Japan	Japan	Tokyo District Court of Japan

* Excluding locations listed separately in this table.

If You are a US State, Local and Education ("SLED") Government end user, these terms, and any disputes arising from them, are subject to the laws of the primary jurisdiction in which You are located in accordance with GSA Schedule Contract Clause 552.238-114 Use of Federal Supply Schedule Contracts by Non-Federal Entities (May 2019).

If You are a US Federal Government end user, these terms, and any disputes arising from them, are subject to the Federal laws of the United States.

13.9 US Government end users

(a) **US SLED Government.** These terms govern all access to Software, Subscription Offers and Documentation by US SLED Government end users. No other rights are granted by Cisco.

(b) **US Federal Government.** The Software, Subscription Offers and Documentation are considered “commercial computer software” and “commercial computer software documentation” under FAR

12.212 and DFARS 227.7202. These terms govern all access to Software, Subscription Offers and Documentation by US Federal Government end users. No other rights are granted by Cisco, but any inconsistency in these terms with federal procurement regulations is not enforceable against the US Federal Government.

13.10 **Notice.** Unless provided in these terms, applicable Offer Description, or an Order, notices to Cisco (a) should be sent to Cisco Systems, Legal Department, 170 West Tasman Drive, San Jose, CA 95134 or by email to contractnotice@cisco.com, and (b) are considered effective (i) upon delivery, if personally delivered, (ii) the next day, if sent by overnight mail, (iii) 3 business days after deposit, postage prepaid, if mailed, or (iv) the same day receipt is acknowledged, if sent by e-mail. Cisco may deliver notice to You under these terms via email or regular mail, but it may provide notices of a general nature applicable to multiple customers on cisco.com.

13.11 **Force majeure.** In accordance with GSAR Clause 552.212-4(f), Neither party is responsible for delay or failure to perform its obligations to the extent caused by events beyond a party’s reasonable control including severe weather events, acts of God, supply shortages, labor strikes, epidemic, pandemic, acts of government, war, acts of terrorism or the stability or availability of utilities (including electricity and telecommunications). The affected party must make commercially reasonable efforts to mitigate the impact of the force majeure event.

13.12 **No waiver.** Failure by either party to enforce any right under these terms will not waive that right.

13.13 **Severability.** If any term in these terms is invalid or unenforceable, then the rest of these terms will continue with full force and effect to the extent possible.

13.14 **Entire agreement.** These terms are the complete agreement between the parties regarding the subject of these terms and replace all previous communications, understandings or agreements (whether written or oral).

13.15 **Translations.** Cisco may provide local language translations of these terms in some locations. Those translations are provided for informational purposes only. If there is any inconsistency in those translations, the English version of these terms will prevail.

13.16 **No publicity.** Neither party will issue any press release or other publications regarding Your use of Cisco Offers without the other party’s advance written permission.

13.17 Order of precedence.

(a) If there is any conflict between these General Terms, Supplemental Terms or any Offer Descriptions, the order of precedence (from highest to lowest) is:

- (1) Regional terms;
- (2) Data Processing Terms;
- (3) Offer Descriptions;
- (4) Supplemental Terms (other than Regional Terms);
- (5) these General Terms; then
- (6) any applicable Cisco policy referenced in these General Terms.

(b) As between You and Cisco, these terms prevail over any inconsistencies with Your contract with any Cisco Partner.

14. Definitions

Term	Meaning
Affiliate	Any corporation or company that directly or indirectly controls, or is controlled by, or is under common control with the relevant party, where “control” means to: (a) own over 50% of the relevant party; or (b) be able to direct the affairs of the relevant party through voting rights or other lawful means (e.g., a contract that allows control).
Approved Source	Cisco, a Cisco Partner, or a fulfillment agent (e.g., public cloud marketplaces) as may be appointed by Cisco from time to time.
Authorized Users	Your users including Affiliates, Your third-party service providers, and each of their respective Users.
Buying Program	Cisco’s consumption-based programs for buying Cisco Offers such as the Cisco Enterprise Agreement.

Cisco Content	Systems Information and data, materials or other content provided by Cisco directly or through Your Approved Source to You as part of Your access to Cisco Offers.
Cisco Offer	Cisco-branded (a) Hardware, (b) Use Rights in Software or Cloud Services, (c) technical support included in a Subscription Offer and (d) incidental technology and resources.
Cisco Partner	A Cisco authorized reseller, distributor, systems integrator or other third party authorized by Cisco to sell Cisco Offers.
Cloud Service	An on-demand service provided by Cisco accessible via the internet and provides software, platform, infrastructure and network products and services on an 'as-a-service' basis as described in the applicable Offer Description.
Term	Meaning
Confidential Information	Non-public proprietary information of the discloser obtained by the recipient in connection with these terms, which: (a) is conspicuously marked as confidential if written or clearly stating the information is confidential when (or promptly after) it is verbally disclosed; or (b) is information which by its nature should reasonably be considered confidential whether disclosed in writing or orally.
Customer Content	As defined in the Data Brief at the Customer Content - Data Brief webpage.
Data	Personal Data, Customer Content and Systems Information.
Data Briefs	Documents describing each type of Data (e.g., Personal Data, Customer Content and Systems Information) that Cisco Offers collect, how it is collected, and when it is used, available at the Trust Portal webpage.
Data Processing Terms	Cisco's data processing terms in the Data Protection Agreement , or terms agreed between You and Cisco covering the same scope.
Documentation	The technical specifications and use materials officially published by Cisco specifying the functionalities and capabilities of the applicable Cisco Offer as updated from time to time.
Free Trial	As defined in section 3.1 (Accessing free trials).
Free Trial Period	As defined in Section 3.1 (Accessing free trials).
Hardware	Tangible Cisco-branded hardware products as generally available on the Price List. Hardware does not include any tangible product listed on the Price List in the name of a third party.
Information Security Exhibit	A document describing the security measures that Cisco implements to secure Personal Data and Customer Content, available at the Information Security Exhibit webpage.
Malicious Code	Code designed or intended to disable or impede the normal operation of, or provide unauthorized access to, networks, systems, Software or Cloud Services other than as intended by the Cisco Offer (e.g., as part of Cisco's security products).
Offer Description	A document published by Cisco as an 'Offer Description' that has more information or related terms specific to a Cisco Offer or Buying Program, available at the Product Specific Terms webpage.
Order	The transaction through which You acquire a Cisco Offer from an Approved Source, including through buying and ordering documents, signing an agreement or statement of work, or transacting through an online ordering tool or marketplace.
Personal Data	Any information about, or relating to, an identifiable individual. It includes any information that can be linked to an individual or used to, directly or indirectly, identify an individual, natural person. Further information regarding Personal Data is on the Personal Data - Data Brief webpage.
Price List	The price lists published at Cisco.com corresponding to the Cisco entity that sells the applicable Cisco Offer.
Privacy Data Sheet	The privacy data sheet applicable to a Cisco Offer available on the Trust Portal - Privacy Data Sheet webpage.
Return	Stopping all use of, destroying or returning applicable Cisco Offers to Your Approved Source, as directed by Cisco or Your Approved Source.
Service Level Agreement	The service level agreement applicable to a Subscription Offer (if applicable) as set out in the applicable Offer Description.
Software	Cisco-branded computer programs, including Upgrades and firmware.
Subscription Offer	Cisco Offers provided on a term, or subscription, basis under Your Order.
Supplemental Terms	Any additional terms applicable to Your Order (including those applying to a specific region or Buying Program).
Systems Information	As defined in the Systems Information – Data Brief webpage.
Transfer Policies	Cisco policies for movement of Use Rights as set out in the Cisco Software Transfer and Re-licensing Policy and the Software License Portability Policy .
Upgrades	All updates, upgrades, bug fixes, error corrections, enhancements and other modifications to the Software.
Use Term	The period You may exercise Use Rights in the Cisco Offer under Your Order.
Use Rights	As set out in section 2.1.

Cisco RMA Policy for Warranty and Hardware Support Contract Returns

Document:

English version File# **EDCS-23258637**

French version File# **EDCS-23258638**

Date: June 2023

Cisco RMA Policy for Warranty and Hardware Support Contract Returns

Cisco Systems, Inc. and its subsidiaries will issue Return Materials Authorization (RMA) numbers to customers to track authorized returns. Any materials returned to Cisco without an authorized RMA will be returned to customer or destroyed at Cisco's option.

Customers must return defective product in accordance with the terms of the product warranty or hardware support contract, as applicable.

If the relevant warranty or support documentation does not provide specific instructions for RMA returns, the terms of this policy apply.

RMA Policy:

Customer must return defective parts in accordance with Cisco's return materials authorization (RMA) procedure located at www.cisco.com within ten (10) calendar days of receipt of the replacement parts. If Customer has not returned the defective parts (which must conform in quantity and serial number to the RMA request) within thirty (30) calendar days of receipt of the replacement parts, Cisco may:

- charge Customer Liquidated Damages equivalent to the full list price (not discounted) of the parts not returned; and
- reduce or deny Advance Replacement Services until the parts are returned or payment for non-return is made.

This policy also applies to returns facilitated by Cisco authorized resellers.

Please follow the packaging instructions and shipping requirements provided on the RMA Process page. You are responsible for the returned parts until we receive them, including any import duties, taxes, and fees.

EDCS-23258637

June 2023

Customer Content



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at <https://www.cisco.com/go/offices>.

 Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Printed in USA

C99-3070973-01 06/23

© 2023 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Page 2 of 2

As part of your use of Cisco solutions, we understand there are times when you will share Customer Content with us. Customer Content means data such as text, audio, video or image files, provided by you to Cisco in connection with your use of Cisco solutions, and data developed at your specific request related to a statement of work or contract. For more examples of Customer Content, see the Examples table below.

Guiding Principles

- **Transparency** – We recognize that your Customer Content shall be treated confidentially and requires separate treatment from Systems Information and other data types.
- **Trusted Ecosystem** – If we are required to share Customer Content to accomplish the purposes for which it was provided to us, then it will only be shared within our trusted ecosystem, meaning the distributors, partners and contractors, as necessary to accomplish those purposes.
- **Customer Control** – Customer Content will be used solely for the purposes you provided it to us for. We will work with you to identify, limit and manage what Customer Content is provided to us.
- **Restricted Data Types** – To the extent that any Customer Content is also considered Personal Data under applicable law or otherwise cannot be separated from Personal Data, we will treat Personal Data according to applicable law and your contracts or agreements with us. For more information on Personal Data, [here](#).

Why we use Customer Content

The following key objectives form a basis on how and when we use and share any Customer Content:

Objective	Summary
1. Solution Delivery	You may provide us with Customer Content so we can provide security threat protection and other solutions. You may also provide Customer Content, such as log, configuration or firmware files, or core dumps, taken from a product and provided to us so we can deliver services such as TAC support, product implementation, business process automation and other services.

1

2. Accelerate Adoption	You may provide us with Customer Content so we may provide you with insights, analytics and recommendations to help you achieve greater value from our solutions to enable your business objectives.
3. Trusted Relationship	You may provide us with Customer Content so that we may assist you with system design, context for troubleshooting, and purchase decisions.
4. Solution Improvements	We do not use Customer Content for solution improvement or development, unless authorized by customer configuration or contract. We use it solely as outlined herein.

Sharing Customer Content

There may be limited reasons for sharing Customer Content. For example, if a product or service you are using includes a hosting or other third party service element, your Customer Content may be hosted or shared with that third party for that reason. These third party contractors will be required to meet our information security requirements before receiving this data. Otherwise, we will not share Customer Content without your prior consent.

Our Information Security Program

We use information security best practices and controls. For further information about how Cisco protects, uses and shares data responsibly, including compliance with applicable laws, data breach notification, data storage, and our data protection requirements, please click [here](#). For information about how we respond to requests for information from governments and courts, please see [here](#).



Personal Data

Examples of Customer Content

The following is a representative, but not exhaustive, list of Customer Content examples:

Examples
Webex Meetings recordings
Cisco and Meraki Smart Camera video recordings
Webex App Space content

Cisco is committed to protecting and respecting Personal Data, no matter where it comes from or where it flows. When we refer to Personal Data (also referred to as Personally Identifiable Information) we mean any information relating to an identified or identifiable natural person (for more information click [here](#)).

Our [Global Personal Data Protection and Privacy Policy](#) demonstrates our commitment to protecting Personal Data and complying with applicable laws regarding Personal Data. In that Policy, we commit to the following principles regarding Personal Data:

- **Fairness.** We will process Personal Data in a lawful, legitimate, and transparent manner.
- **Purpose Limitation.** We will only collect Personal Data for specific, explicit, and legitimate purposes. Any subsequent processing should be compatible with those purposes, unless we have obtained the individual's consent, or the processing is otherwise permitted by law.
- **Proportionality.** We will only process Personal Data that is adequate, relevant, and not excessive for the purposes for which it is processed.
- **Data Integrity.** We will keep Personal Data accurate, complete, and up-to-date as is reasonably necessary for the purposes for which it is processed.
- **Data Retention.** We will keep Personal Data in a form that is personally identifiable for no longer than necessary to accomplish the purposes, or other permitted purpose(s), for which the Personal Data was obtained.
- **Data Security.** We will implement appropriate and reasonable technical and organizational measures to safeguard Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure, use, or access. We will instruct and contractually require third parties processing Personal Data on behalf of Cisco, if any, to: (a) process it only for purposes consistent with Cisco's purposes for processing; and (b) implement appropriate technical and organizational measures to safeguard the Personal Data.
- **Individual Rights.** We will process Personal Data in a manner that respects individuals' rights under applicable data protection laws.

- **Accountability.** We will implement appropriate governance, policies, processes, controls, and other measures necessary to enable it to demonstrate that its processing of Personal Data is in accordance with our Global Personal Data Protection and Privacy Policy and applicable data protection laws.

Why we process Personal Data

The following key objectives form the basis of how and when we use Personal Data:

Objective	Summary
Solution Delivery	Personal Data may be used to operate our products and deliver services to you with critical and timely system insights. For example, our Cloud offers depend on proper user authentication. Personal Data is also needed for us and our partners to provide you with warranty support, technical support and other services.
Accelerate Adoption	Our products and services contain various features that you can employ to best address your business objectives. We work closely with your organization to accelerate your time to realize the value of our products and services, provide consultation, recommendations, expert insights, analysis and training so you can best utilize the many features of our products and services in a way that best meets your needs.
Trusted Relationship	We view ourselves as a trusted advisor to you and maintain a number of relationships within your organization. We need these contacts for a number of purposes, such as to advise and guide you in your buying decisions, to keep you up to date on renewals, and to ultimately help you transact business with us and your partners or distributors (if any).
Solution Improvements	Our solutions must evolve and improve to meet our customers' changing needs. These improvements are guided by the insights gained from Systems Information that show us how our solutions are working and being used. If Personal Data is received in connection with Systems Information, we will treat that data as you would expect - as Personal Data, not as Systems Information - and always consistent with applicable law and your contracts or agreements with us.

Our Privacy Data Sheets and Privacy Data Maps

We maintain Privacy Data Sheets and Privacy Data Maps on the [Cisco Trust Portal](#) for specific products and services that provide you with additional information such as what Personal Data we process, where and for how long we store the information, and what sub-processors we may use.

Our Data Protection Agreement

When Cisco is acting as data processor (i.e., managing Personal Data on behalf of our customers), our Data Protection Agreement (DPA), applicable Privacy Data Sheets and our Online Privacy Statement provide details about our commitments regarding our processing of Personal Data when you use our products and services. Our DPA is publicly available on the Cisco Trust Center ([here](#)). Key elements in the DPA include:

- terms and conditions consistent with the principles in this document that will govern the processing of Personal Data;
- technical and organizational security measures that will be implemented to minimize the risk of accidental loss, destruction, alteration, unauthorized disclosure, unauthorized access, or unlawful destruction of Personal Data; and
- incorporation of the European Union Standard Contractual Clauses, and APEC Cross Border Privacy Rules system requirements for international data transfers.

Our Online Privacy Statement

When you access our websites or use one of our solutions, our [Online Privacy Statement](#) describes how we handle Personal Data and provides the choices available to you regarding our collection, use, and access to that information.

Sharing Personal Data

We require our suppliers and contractors to adhere to applicable data protection laws and terms and conditions consistent with the principles in this document when handling Personal Data on our behalf by signing our Supplier DPA, which is publicly available [here](#).

Similarly, we require all of our partners and distributors to comply with applicable laws, including privacy and data protection laws, and the confidentiality provisions in our agreement with them.

How Individuals can control their Personal Data

We respect the rights of individuals regarding their Personal Data. We provide a [Cisco Profile Management Tool](#) that allows you to view, edit and set the preferences related to the Personal Data in for your Cisco profile. We also provide a [Privacy Request Form](#) to assist you and your end users with any inquiries about your Personal Data and process requests, such as to opt-out from communications etc.

Our Information Security Program

We maintain a robust Information Security Program. For detailed information, please click [here](#).

Data Transfer Mechanisms

We have invested in the following transfer mechanisms when transferring Personal Data across jurisdictions:

- [EU Standard Contractual Clauses](#)
- [Binding Corporate Rules](#) for Controllers
- Binding Corporate Rules for Processors (pending approval)
- [APEC Cross Border Privacy Rules](#)
- [APEC Privacy Recognition for Processors](#)

Breach Notification Processes

The Data Protection & Privacy team within Cisco's Security & Trust Organization coordinates the Data Incident Response Process and manages the enterprise-wide response to data-centric incidents. Our Incident Commander directs and coordinates our response, using diverse teams including the Cisco Product Security Incident Response Team (PSIRT), the Cisco Security Incident Response Team (CSIRT), and the Advanced Security Initiatives Group (ASIG). For additional information regarding our breach notification process, please see Cisco's DPA [here](#).

Systems Information

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

In order to give you, our customers, the full value of your Cisco products and services, we receive and use certain technical data and information about the operation and performance of your Cisco solutions, which we refer to as Systems Information. **Systems Information** means data generated or collected in connection with your use and operation of Cisco solutions, and data provided by you in connection with our delivery of products and services to you (including, for example, when you submit a request related to support services). Systems Information is composed of Telemetry Data, Support Data, Install Base Information, Entitlement Information, Customer Feedback and Security Threat Data, as defined further below.

Guiding Principles

- **Transparency** – We only use Systems Information for the purposes set out in the objectives noted below.
- **Trusted Ecosystem** – Systems Information that can be attributable to you is only shared within our trusted ecosystem, meaning the partners, distributors and contractors who help provide our solutions to you and who are also committed to protecting that data.
- **Customer Control** – There are certain products and services that require Systems Information in order to function and provide the solution to you. We will be transparent about these requirements so you may then choose whether or not to install or use the product, service or specific feature that requires that access. For other products and services, you may have the option to configure whether Systems Information is shared with us or the ability to decline our requests to provide Systems Information to us.
- **Restricted Data Types** – We recognize and respect that your Personal Data (also referred to as Personally Identifiable Information) and Customer Content are especially sensitive and require separate treatment specific to those data types. If any such Personal Data or Customer Content is incidentally received, we will treat that data as you would expect - as Personal Data or Customer Content, not as Systems Information - and always consistent with applicable law and your contracts or agreements with us. For more information on Personal Data, please see [here](#). For more information about Customer Content, please see [here](#).

How we use Systems Information

The following key objectives form the basis of how and when we use Systems Information:

Objective	Examples
1. Solution Delivery	Systems Information is used to operate our products and deliver services to you with critical and timely system insights, as well as to provide you with warranty coverage, technical support and similar services.
2. Accelerate Adoption	Systems Information is used to derive insights and analytics to help you achieve greater value from our solutions to enable your business objectives. These insights and analytics are critical to provide you with network consultation, recommendations, expert insights, analysis and training so you can utilize our products and services in a way that best meets your needs, improves your user experiences and applies a customerfocused quality of service.
3. Trusted Relationship	Systems Information is used to help us ensure that you receive what you purchased or are entitled to, including managing subscription renewals, validating and managing entitlement, trial use and similar activities. We also rely on Systems information to help enhance our relationships with you.
4. Solution Improvements	Our solutions must evolve and improve to meet our customers' changing needs. Systems Information is used to gain insights that show us how our solutions are working and being used. Based on these insights, we use Systems Information to modify and improve our solutions, as well as to develop new solutions.

For examples of how we use Systems Information to meet these key objectives, see [Table 2](#) below.

How we collect and generate Systems Information

We collect and generate Systems Information in a variety of ways, and we use this Systems Information solely to meet the objectives stated above. There are some products and services that require Systems Information to properly or fully function. There are other purchase arrangements, such as utility billing arrangements, that require us to collect Systems Information to determine usage. If you choose not to provide us with Systems Information, it may limit or prevent our ability to deliver the solutions you purchased and related advanced feature functions, security capabilities, services and other insights and analytics.

Systems Information Generated by our Products and Services

We may receive Systems Information from some of our products and services that generate Systems Information in the ordinary course of use (including, for example, by our instrumentation and logging systems).

Systems Information Collected by our Data Collection Tools

When you purchase and use certain Cisco products and services, we collect Systems Information through the use of data collection tools and related tools, such as Cisco's Common Services Platform Collector software, Cisco Software Subscription Manager, onsite hardware appliances, cloud-based software, or third party network collectors. When you install a data collection tool in your network, it securely communicates with network devices and directly transmits Systems Information back to us. While it is ultimately your choice whether or not to install and activate these data collection tools in your environment, these tools may be necessary and critical to providing services to you and operating products in your network.

Systems Information Provided by You

We sometimes receive Systems Information directly from you as part of our delivery of products and services. For instance, we may receive Support Data (as described in Table 1 below) and other Systems Information from you about the Cisco or third party products and solutions deployed in your network so we can provide support services, or help you plan, design, implement and optimize your network, etc.

How we share Systems Information

We sometimes need to share Systems Information with our trusted ecosystem of partners, distributors and contractors. If you purchase a solution through a Cisco partner, we may provide your partner or its distributor with the System Information needed to deliver and perform that solution, manage your subscription, and fulfill subscription billing and administrative activities, consistent with the objectives described above. We may also contract with service providers and share Systems Information necessary to operate and service our solutions. In each instance, each participant in our trusted ecosystem has agreed to confidentiality, applicable law and other requirements with us that are consistent with our commitments to you.

If the Systems Information does not identify a specific customer, such as when the Systems Information is effectively de-identified, then we may freely use and share Systems Information and related insights and analytics.

Data Protection and Information Security

We use information security best practices and controls to protect data in our possession. For further information about how Cisco protects, uses and shares data responsibly, including compliance with applicable laws, data breach notification, data storage, and our data protection requirements, please see [here](#). For information about how we respond to requests for information from governments and courts, please see [here](#).

Definitions and Examples

Table 1. Systems Information

Systems Information Sub-Categories	Definitions and Examples
---------------------------------------	--------------------------

Telemetry Data	Data generated by instrumentation and logging systems created through the use and operation of the product or service. Examples: • <i>Product Identification</i>. Cisco product serial numbers and other identification information. Information characterizing devices connected to a network. • <i>Sensor Data</i>. Data generated by sensors, devices and machinery, product or service features or functionality activated, accessed or utilized. • <i>Configuration Data</i>. Network policy, hardware module and software components installed, connections and topology relationships between products. • <i>Cookies and Beacons</i>. Data relating to the existence of cookies, web beacons, and other similar applications. • <i>Application Information</i>. The types of Cisco software or applications installed on a network or device. • <i>Network, Software and Cloud Traffic</i>. Data related to the usage, origin of use, traffic density and patterns. Behavior of workloads, and applications across a network or cloud service.
Support Data	Data we collect when you submit a request for support services or other troubleshooting, including information about hardware, software and other details related to the support incident.
Install Base Information	Types, quantities and location of installed Cisco devices, products, or software releases.
Entitlement Information	Software license, warranty, cloud and service subscription information.
Customer Feedback	Technical data or suggestions contained in oral or written communications you provide us regarding modifications or improvements to a product or service.
Security Threat data	Threat intelligence data, URLs, metadata, net flow data, origin and nature of malware and other information necessary to enable security features of a product or service.

Table 2. Objectives

The following is a representative, but not exhaustive, list of the objectives for which we use Systems Information:

Objective	Examples
Solution Delivery	• Critical support actions, recommendations. Reactive, Proactive and Predictive problem detection and remediation, insights and analytics. • Automation and orchestration of lifecycle services: migration, development, test, release, operations. Solution integration to customer business and IT processes.

Accelerate Adoption	• Product usage, feature usage, application interaction, • Selecting relevant learning and training content. • Planning and readiness for new technology evaluation and deployment • Recommendations to maximize solution value and return on investment.
Trusted Relationship	• Support coverage, and entitlement assurance and renewal eligibility. • Notification of known product security vulnerabilities, field notices and bugs • Verification of system integrity, authentic system hardware signature and signed/ encrypted software signatures. • Recommendations regarding changes to or new products and services.
Solution Improvements	• Product innovation, software updates, development of new features and offers, threat intelligence detection improvements. • Serviceability and product quality improvements aligned to customer satisfaction.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.



Data Protection Agreement

Applies to Customer's Personal Data

This Data Protection Agreement ("**DPA**"), forms part of the Agreement (as defined below) and applies where, and to the extent that, Cisco Processes Personal Data as a Processor for You when providing Cisco Offers (as defined below) under the Agreement, (each a "**Party**" and together the "**Parties**").

This DPA will become effective on the Effective Date and remain in force for the term of Agreement.

Unless otherwise specified in this DPA, the terms of the Agreement will continue in full force and effect. All capitalized terms not defined in Section 1 or otherwise in this DPA will have the meanings set forth in the Agreement. Any privacy or data protection related clauses or agreement previously entered into by Cisco and You, with regards to the subject matter of this DPA, will be superseded by and replaced with this DPA. No one other than a Party to this DPA, their successors and permitted assignees will have any right to enforce any of its terms.

If the Customer is an Ordering Activity under GSA Schedule Contracts, it shall only be required to comply with the Federal law of the United States and expressly does not agree to comply with any provision of this Data Processing Agreement, EU Law, or law of an EU Member State that is inconsistent with the Federal law of the United States.

1. Definitions

- 1.1. "**Affiliates**" means, any corporation or company that directly or indirectly controls, or is controlled by, or is under common control with the relevant party, where "control" means to: (a) own over 50% of the relevant party; or (b) be able to direct the affairs of the relevant party through voting rights or other lawful means (e.g., a contract that allows control). Unless otherwise explicitly agreed by the Parties, any legal entities which become part of the Cisco group of companies through an acquisition or merger (each an "**Acquired Entity**") are not considered Cisco Affiliates for the purposes of this DPA unless the Cisco Offers of such Acquired Entity are available for You to purchase on the applicable Price List.
- 1.2. "**Agreement**" means the written or electronic agreement between You and the applicable Cisco entity for the provision of the Cisco Offers to You or any other terms where the parties expressly agree to this document (e.g.: the Cisco General Terms ("**General Terms**")); or where You have purchased a Cisco Offer from a Cisco partner, "Agreement" means, for the purposes of this DPA only, the applicable Service Description listed at <https://www.cisco.com/c/en/us/about/legal/service-descriptions.html>.
- 1.3. "**APEC**" means the Asia Pacific Economic Cooperation, a regional economic forum established in 1989 to leverage the growing interdependence of the Asia-Pacific. See <http://www.apec.org> for more information.
- 1.4. "**APEC Member Economy**" means the 21 members of APEC: Australia, Brunei Darussalam, Canada, Chile, China, Hong Kong-China, Indonesia, Japan, Republic of Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, Philippines, Russia, Singapore, Chinese Taipei, Thailand, United States, and Vietnam.
- 1.5. "**Approved Jurisdiction**" means a member state of the EEA, or other jurisdiction approved as having adequate legal protections for data by the European Commission, currently found here: <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy>https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.
- 1.6. "**Cisco**" means the applicable Cisco entity that is party to the Agreement.

- 1.7. **“CCPA”** means the California Consumer Privacy Act (Cal. Civ. Code §§ 1798.100 to 1798.199) as amended by the California Privacy Rights Act (“CPRA”), and any related regulations or guidance provided by the applicable regulators.
- 1.8. **“Cisco Offer”** means Cisco branded (a) hardware, (b) usage rights in software or cloud services, (c) technical support included in a subscription offer and (d) incidental technology and resources acquired by You.
- 1.9. **“Controller”** means an entity that determines the purposes and means of the processing of Personal Data. It will have the same meaning ascribed to “controller” under the GDPR and other equivalent terms under applicable Data Protection Laws (e.g.: “Business” as defined under the CCPA), as applicable.
- 1.10. **“Customer” or “You”** means the Party identified in the Agreement receiving Cisco Offers from Cisco under the Agreement.
- 1.11. **“Data Breach”** means a breach of the Information Security Exhibit leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data.
- 1.12. **“Data Protection Laws”** means all mandatory applicable laws that apply to the Processing of Personal Data under the Agreement.
- 1.13. **“Data Subject”** means the individual to whom Personal Data relates (e.g.: “Consumer” as defined under the CCPA).
- 1.14. **“EEA”** means those countries that are members of the European Economic Area.
- 1.15. **“GDPR”** means Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons regarding the processing of Personal Data and on the free movement of such data (General Data Protection Regulation).
- 1.16. **“Information Security Exhibit”** means the document describing the measures that Cisco implements to secure Personal Data, which can be found [here](#).
- 1.17. **“Personal Data”** means any information about, or related to, an identified or identifiable natural person Processed by Cisco and/or its Affiliates on behalf of You. It includes any information that can be linked to an individual or used to directly or indirectly identify an individual, natural person.
- 1.18. **“Price List”** means the price lists published at Cisco.com corresponding to the Cisco entity that sells the applicable Cisco Offer.
- 1.19. **“Privacy Data Sheet(s)”** means the applicable document located on Cisco’s [Trust Portal](#) that describes the Processing activities in relation to the Cisco Offer(s) supplied to You under the Agreement. If a Privacy Data Sheet is attached to or referenced in this DPA, this DPA only refers to Cisco’s role as a Processor as detailed in the respective Privacy Data Sheet, unless the Parties have explicitly agreed otherwise herein.
- 1.20. **“Processing”** means any operation or set of operations that is performed upon Personal Data, whether or not by automatic means, such as collection, recording, securing, organization, storage, adaptation or alteration, access to, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction. **“Processes”** and **“Process”** will be construed accordingly.
- 1.21. **“Processor”** means an entity that processes Personal Data on behalf of a Controller. It will have the same meaning ascribed to “processor” under the GDPR and other equivalent terms under other Data Protection Laws (e.g.: “Service Provider” as defined under the CCPA), as applicable.
- 1.22. **“Representatives”** means either Party’s (including its Affiliates’) officers, directors, employees, agents, contractors, temporary personnel, subcontractors and consultants.

- 1.23. **“Subprocessor”** means another Processor engaged by Cisco to carry out Processing of Your Personal Data, as set forth in the applicable Privacy Data Sheet(s).

2. Processing of Personal Data

- 2.1. The Parties agree that, for this DPA, (i) You will be the Controller and Cisco will be the Processor and/or (ii) You will be the Processor and Cisco will be a further Processor.
- 2.2. Cisco Processes Personal Data as part of this DPA as follows:
- a. The duration of the Processing under this DPA is determined by You and as set forth in the Agreement.
 - b. The purpose of the Processing under DPA is the provision of the Cisco Offers by Cisco to You as specified in the Agreement and as further detailed in the respective Privacy Data Sheet(s).
- 2.3. You will:
- a. use the Cisco Offers in compliance with Data Protection Laws;
 - b. ensure all instructions given by it to Cisco in respect of the Processing of Personal Data are at all times in accordance with Data Protection Laws;
 - c. ensure all Personal Data provided to Cisco has been collected in accordance with Data Protection Laws and that You have all authorizations and/or consents necessary to provide such Personal Data to Cisco;
 - d. keep the amount of Personal Data provided to Cisco to the minimum necessary for the provision of the Cisco Offers;and
 - e. when acting as a Processor, be responsible for passing on to the Controller all the information, assistance and notices needed to comply with its obligations as a Controller under Data Protection Laws, as well as the details of the applicable Privacy Data Sheets, given that You are the Party having a direct relationship with the Controller; and be responsible for passing on to Cisco all Controller’s requests and instructions related to the Processing of Personal Data under this DPA.
- 2.4. Cisco will:
- a. only Process Personal Data in accordance with Data Protection Laws and Your documented instructions, the applicable Privacy Data Sheet(s), the Information Security Exhibit, and this DPA. Cisco will promptly notify You if Cisco reasonably believes that Your instructions are inconsistent with Data Protection Laws;
 - b. ensure its applicable Representatives who may Process Personal Data have written contractual obligations in place with Cisco to keep the Personal Data confidential or are under an appropriate statutory obligation of confidentiality;
 - c. appoint data protection lead(s). Upon request, Cisco will provide the contact details of the appointed person(s);
 - d. assist You as reasonably needed to respond to requests from supervisory authorities, Data Subjects, customers, or others to provide information related to Cisco’s Processing of Personal Data;
 - e. if required by Data Protection Laws, court order, subpoena, or other legal or judicial process to Process Personal Data other than in accordance with Your instructions, notify You without undue delay of any such requirement before Processing the Personal Data (unless mandatory applicable law prohibits such notification, in particular on important grounds of public interest);
 - f. maintain records of the Processing of any Personal Data received from You under the Agreement;
 - g. not lease, sell, distribute, or otherwise encumber Personal Data unless mutually agreed to by the Parties in a separate agreement;
 - h. not combine Personal Data received from or on behalf of You and Personal Data collected by Cisco’s own interactions with the Data Subject other than as provided in the Agreement or as otherwise permitted by Data Protection Laws;

- i. provide such assistance as You reasonably require (either on its own behalf or on behalf of its customers), and Cisco or a Representative is able to provide, in order to meet any applicable filing, approval or similar requirements in relation to Data Protection Laws;
- j. provide such information and assistance as You reasonably require (taking into account the nature of Processing and the information available to Cisco) to enable Your compliance with Your obligations under Data Protection Laws with respect to: i. security of Processing; ii. data protection impact assessments (as such term is defined by the GDPR); iii. prior consultation with a supervisory authority regarding high-risk Processing; and iv. notifications to the applicable supervisory authority and/or communications to Data Subjects by You in response to any Data Breach;
- k. on termination of the DPA for whatever reason, cease to Process Personal Data, and upon Your written request and without undue delay, (i) return, or make available for return, Personal Data in its possession or control, or (ii) securely delete or permanently render unreadable or inaccessible existing copies of the Personal Data; unless continued retention and Processing is required or is permitted by Data Protection Laws and/or mandatory applicable law. At Your request, Cisco will give You confirmation in writing that it has fully complied with this Section 2.4 (k) or provide a justification as to why such compliance is not feasible.

3. Transfers of Personal Data

Cisco may transfer and Process Personal Data to and in locations where Cisco or its Subprocessors Process Personal Data to provide the Cisco Offers, as further detailed in the respective Privacy Data Sheet(s). Cisco will conduct such transfers in accordance with the transfer mechanisms set out at Cisco's [DPA Portal](#). Any further changes to such transfer mechanisms approved with an official decision by the applicable competent authority will be incorporated by reference to this DPA and a copy of the new transfer mechanism will be available at Cisco's DPA Portal.

4. Subprocessing

- 4.1. Where Cisco appoints a Subprocessor, Cisco will execute a written agreement with the Subprocessor containing terms at least as protective as this DPA. Current Subprocessor(s) are listed in the applicable Privacy Data Sheet(s).
- 4.2. Cisco will not subcontract its obligations under this DPA to new Subprocessors, in whole or in part, without providing You with notice (e.g.: by publishing this information at Cisco's [Trust Portal](#) and/or by email upon Your subscription at Cisco's [Trust Portal](#)) and an opportunity to object. If within 10 days of Cisco's notice, You object to the proposed subcontracting by providing reasonable grounds related to the protection of the Personal Data and the Parties cannot resolve the objection within 30 days of Cisco's notice, then You may on written notice, terminate the applicable part of the Agreement and/or purchase order relating to those Cisco Offers which cannot be provided by Cisco without the use of the Subprocessor(s) giving rise to the objection.
- 4.3. Cisco will be liable for the acts or omissions of Subprocessors to the same extent it is liable for its own actions or omissions under this DPA.

5. Rights of Data Subjects

Data Subject requests. To the extent legally permitted, Cisco will promptly redirect the Data Subjects to send their requests to You or notify You if it receives a Data Subject request. Unless required by Data Protection Laws, Cisco will not respond to any such Data Subject request without Your prior written consent except to redirect the Data Subject request to You. Cisco will provide such information and cooperation and take such action as You reasonably request in relation to a Data Subject request.

6. Security

Controls for the protection of Personal Data. Cisco will implement and maintain the security measures specified in the Information Security Exhibit and regularly monitor compliance with these security measures.

7. Audit

Upon Your written request, and subject to the confidentiality obligations set forth in the Agreement, Cisco will make available to You reasonably necessary information to demonstrate Cisco's compliance with the obligations of this DPA and Data Protection Laws, in accordance with the Information Security Exhibit.

8. Notification and Communication

- 8.1. Notification. Cisco will notify You within 48 hours of confirmation of a Data Breach relating to Your Personal Data. Cisco will provide all such timely information and cooperation as You may reasonably require for You to fulfil Your Data Breach reporting obligations under (and in accordance with the timescales required by) Data Protection Law. Cisco will further take such measures and actions as it considers necessary or appropriate to remedy or mitigate the effects of the Data Breach and will keep You informed in connection with the Data Breach.
- 8.2. Information Security Communication. Except as required by mandatory applicable law, Cisco agrees that it will not inform any third party of a Data Breach referencing or identifying You, without Your prior written consent. Cisco will reasonably cooperate with You and law enforcement authorities concerning a Data Breach. Cisco will retain, for an appropriate period of time, all information and data within Cisco's possession or control that is directly related to any Data Breach. If disclosure of the Data Breach referencing or identifying You is required by mandatory applicable law, Cisco will work with You regarding the timing, content, and recipients of such disclosure.
- 8.3. Post-incident. Cisco will reasonably cooperate with You in any post-incident investigation, remediation, and communication efforts.
- 8.4. Complaints or notices related to Personal Data. If Cisco receives any official complaint, notice, or communication that relates to Cisco's Processing of Personal Data or either Party's compliance with Data Protection Laws in connection with Personal Data, to the extent legally permitted, Cisco will promptly notify You and, to the extent applicable, Cisco will provide You with commercially reasonable cooperation and assistance in relation to any such complaint, notice, or communication.

9. Liability

- 9.1. Each Party's respective direct liability to Data Subjects or applicable supervisory data protection authorities which cannot be limited or excluded by mandatory applicable law will be unlimited.
- 9.2. Except for any liability which cannot be limited or excluded under mandatory applicable law, the aggregate liability of Cisco for all Data Breaches and any breach of this DPA (whether for breach of contract, misrepresentations, negligence, strict liability, other torts or otherwise) will not exceed US\$1,000,000.
- 9.3. Where a Data Breach and/or breach of this DPA is also a breach of any confidentiality or non-disclosure obligations in the Agreement, the liability cap in Section 9.2 will apply.



Information Security Exhibit

1. **Scope.** This Information Security Exhibit ("**ISE**") describes the technical and organizational security measures that Cisco will use to protect Your Data that we process while providing Cisco Offers to You under the Agreement. This ISE applies to any Cisco Offer that is on Cisco's Global Price List, except where an Offer Description describes or references an alternative set of security measures that Cisco will use to protect Your Data.
2. **General.** Cisco will use reasonable and appropriate technical and organizational security measures designed to protect the security of Your Data. Those measures are described in this Information Security Exhibit (the "**Security Measures**"). Cisco may change the Security Measures in its sole discretion, so long as Cisco reasonably determines that the changes do not materially reduce the overall level of protection the Security Measures provide.

3. Technical and Organizational Security Measures.

3.1. Information Security Program.

- a. **General.** Cisco will implement and maintain a written information security program, consisting of a set of policies, standards, procedures, and other controls aimed at protecting the security of Your Data (the "**Information Security Program**"). Cisco's Information Security Program will be based on one or more internationally recognized information security frameworks (e.g., SOC 2, ISO 27001, etc.).
- b. **Security Ownership.** Cisco will appoint one or more managers who will be responsible for coordinating and monitoring the Information Security Program. These managers have responsibility and accountability for information security within the organization and will have the knowledge, experience, and authority to perform this function.
- c. **Security Roles and Responsibilities.** Cisco's Information Security Program will include policies and procedures for defining and assigning roles and responsibilities pertaining to information security.
- d. **Review of Information Security Program.** Cisco will conduct periodic reviews of its approach to managing information security risks through internal and/or external assessors.
- e. **Compliance Reviews.** Cisco will perform periodic assessments of its compliance with Cisco's information security policies and standards through internal and/or external assessors.

3.2. Human Resources Security.

- a. **Confidentiality.** Cisco Personnel with access to Your Data will be subject to confidentiality obligations.
- b. **Training.** Cisco Personnel will undertake awareness training regarding Cisco's privacy and security policies. This training will be: (i) provided as part of the onboarding process when Cisco Personnel are first employed or engaged by Cisco, whichever the case may be, and (ii) periodically (but at least annually) refreshed through means such as training courses, emails, posters, notice boards, and/or other training and awareness materials. Cisco will inform its personnel of the possible consequences of breaching Cisco's security policies and procedures, including possible termination of employment or assignment.
- c. **Background Checks.** Where permitted by law, Cisco will perform background checks, including criminal background checks, on Cisco Personnel pursuant to Cisco's policies.

3.3. Access Controls.

- a. **Access Restrictions.** Cisco will maintain policies and procedures for restricting Cisco Personnel's access to Your Data based on the principles of least privileged access and on a need-to-know basis.

- b. **Suspension or Termination of Access.** Cisco will maintain policies and procedures regarding the invalidation of access credentials for Cisco Personnel: (i) in connection with the termination of employment or assignment, in the case of an employee or contingent worker, respectively, or (ii) in the event Cisco determines that the confidentiality of the access credentials has been compromised.

- c. **Access Reviews.** Cisco will maintain policies and procedures for periodically reviewing access privileges granted to Cisco Personnel.

- d. **Authentication.**
 - i. **Password Requirements.** Where Cisco Personnel are required to log in to Information Systems using passwords, Cisco will maintain policies and procedures that address strong password control parameters (e.g., length, character complexity, and/or non-repeatability), requirements for Cisco Personnel to change default passwords, and monitoring of multiple failed login attempts.
 - ii. **Assignment of Credentials.** Cisco will prohibit multiple Cisco Personnel from being assigned the same user ID/username.
 - iii. **Administration of Access.** Cisco will maintain policies that restrict the administration (i.e., granting, modification, and revocation) of access privileges to authorized personnel.
- e. **Remote Access.**
 - i. **General.** Cisco will require Cisco Personnel to authenticate their identity using multi-factor authentication when accessing the Cisco corporate network from remote locations.
 - ii. **Virtual Private Networks (“VPN”).** When Cisco Personnel use Cisco’s corporate VPN to remotely connect to Cisco’s corporate network for the processing of Your Data: (i) the VPN connections will be encrypted using industry standard cryptography; (ii) VPN connections will only be established using VPN servers; and (iii) the use of multi-factor authentication will be required.
 - iii. **Zero Trust.** When Cisco Personnel use Cisco’s zero trust architecture to remotely connect to Information Systems, the following requirements will be met: (i) Cisco Personnel accessing the relevant Information System will use a Cisco-managed endpoint; (ii) the managed endpoint will satisfy the device configuration requirements (e.g., required operating system versions) that Cisco requires the endpoint to have in place prior to accessing the relevant Information System; and (iii) multi-factor authentication will be used for Cisco Personnel to access the relevant Information System.

3.4. Physical Security.

- a. **Physical Access to Facilities.** Cisco will implement and maintain the following controls designed to restrict physical access to Facilities to authorized individuals:
 - i. Facilities will be monitored, such as through the use of CCTV or onsite security, 24 hours a day, seven days per week.
 - ii. Access to Facilities will be controlled through electronic access controls (e.g., key card, key fob, etc.) and/or sign-in procedures.
 - iii. Authorized visitors to the Facilities will be required to sign-in, carry identification badges and be escorted.

- b. **Clean Desk and Clear Screen Policies.** Cisco will maintain clean desk and clear screen policies.

- c. **Environmental Measures.** Cisco's data centers will have: (i) backup generators or other secondary power supplies; (ii) temperature and humidity controls for heating, ventilation, and air conditioning (HVAC) equipment; and (iii) fire detection and suppression systems.
- 3.5. Change Management.**
 - a. **Change Management Policy.** Cisco will maintain a documented change management policy. The change management policy will describe roles and responsibilities to support separation of duties (e.g., request, approve, implement).
 - b. **Change Management Procedure.** Cisco will maintain change control procedures for monitoring and implementing changes to production systems, networks, applications, and data file structures.
- 3.6. Logging and Monitoring.** Cisco will maintain policies and procedures related to logging and monitoring of certain events related to the Information Systems, such as administrator and operator login activity.
- 3.7. Network Security.** Cisco will implement technical measures on the Cisco corporate networks used to process Your Data, such as firewalls, segmentation, distributed denial-of-service mitigation, network flow analysis, and domain name service (DNS) security.
- 3.8. System Acquisition, Development, and Maintenance.**
 - a. **Security Requirements.** Cisco will maintain documented security requirements for the purchase, use, or development of Information Systems.
 - b. **Development Requirements.** Cisco will maintain policies for secure development, system engineering, and support. Cisco will conduct system security testing as part of the development lifecycle process. Cisco will supervise and monitor the activity of outsourced system development.
- 3.9. Cryptography.** Cisco will maintain policies that cover the use of cryptographic technologies, including key and certificate lifecycle management, cryptographic algorithms, and cryptographic strength (e.g., key length).
- 3.10. Vulnerability Management and Penetration Testing.**
 - a. **Policies and Procedures.** Cisco will maintain vulnerability management policies and procedures.
 - b. **Scanning and Testing.** Cisco will perform periodic vulnerability scans and penetration tests of the Cisco corporate network used to process Your Data. Penetration tests will be conducted by qualified professionals, which may include internal testers and/or third-party testers, using industry standard tools and methodologies.
 - c. **Assessment of Vulnerabilities and Remedial Action.** If any penetration test or vulnerability scans referred to in Section 3.10(b) reveals material vulnerabilities, Cisco will assess the vulnerabilities and take such steps for addressing these vulnerabilities that Cisco reasonably determines to be necessary.
- 3.11. Incident Management.** Cisco will maintain an information security incident response program, including documented procedures for investigating and addressing information security incidents. The information security incident response program will address topics such as prioritization of incidents, roles and responsibilities, internal escalation procedures, tracking and reporting, and containment and remediation. The information security incident management program will be tested, reviewed, and approved on a periodic basis.
- 3.12. Supplier Risk Management.**
 - a. **Policies.** Cisco will have vendor management policies and procedures that are designed to impose cybersecurity obligations upon its Suppliers that are no less protective for Your Data than those obligations imposed upon Cisco by this Information Security Exhibit to the extent such obligations are applicable given the nature of the services provided by the Supplier.
 - b. **Security Assessments.** Cisco will assess its Suppliers' security practices against the security requirements set forth in Cisco's agreements with such Suppliers.
- 3.13. Business Continuity and Disaster Recovery.** Cisco will maintain business continuity and disaster recovery plans for its Facilities. Cisco will review and test those plans periodically, but no less than annually.

3.14. Audits and Certifications. Cisco will make available to You copies of third-party audit reports or certifications it maintains in the ordinary course of business (such as SOC1, SOC2, SOC3 attestations, or ISO 27001:2013 certifications (or their equivalent under any successor standards)) that apply to the relevant Cisco Offer (“**Audit Reports**”). Additionally, if Your audit requirements under Data Protection Laws cannot be reasonably satisfied by the Audit Reports and other information that Cisco generally makes available to You, Cisco will cooperate with reasonable requests by You to audit Cisco’s compliance with this Information Security Exhibit. This cooperation will be to the extent reasonably necessary to satisfy such obligations under Data Protection Laws and subject to mutual agreement on time, duration, place, scope and manner of the audit. You will treat the contents of the Audit Reports and any information obtained by You in connection with any other audit performed under this Section 3.14 as Cisco’s confidential information.

4. **Your Responsibility.** While Cisco is responsible for performing its obligations under this Information Security Exhibit, You are solely responsible for using the security features and functionalities that Cisco makes available to You and for ensuring Your use of Cisco Offers complies with Your security requirements and applicable laws, including Data Protection Laws.

5. **Definitions.**

Term	Meaning
Affiliate	Any corporation or company that directly or indirectly controls, or is controlled by, or is under common control with the relevant party, where “control” means to: (a) own over 50% of the relevant party; or (b) be able to direct the affairs of the relevant party through voting rights or other lawful means (e.g., a contract that allows control).
Agreement	The written or electronic agreement between You and Cisco or the applicable Cisco Affiliate for the provision of the Cisco Offer.
Cisco, We	Cisco Systems, Inc. or its applicable Affiliates.
Cisco Offer	Cisco-branded (a) hardware, (b) software, (c) Cloud Services and other services (including technical support included in a Subscription Offer) and (d) incidental technology and resources.
Cisco Personnel	Cisco’s employees and contingent workers who have access to Your Data.
Cloud Service	An on-demand service provided by Cisco accessible via the internet that provides software, platform, infrastructure and network products and services on an ‘as-a-service’ basis as described in the applicable Offer Description.
Customer Content	As defined in the Data Brief at Customer Content – Data Brief .
Data Protection Laws	All applicable privacy/data protection laws that apply to the processing of Personal Data under the Agreement.
Facilities	The data centres and portions of the Cisco corporate office buildings where Cisco stores the corporate servers and network infrastructure that it uses to process Your Data during the course of providing Cisco Offers to You.
Information Systems	An information system that Cisco uses to process Customer Content and Personal Data.
Offer Description	A document published by Cisco as an ‘Offer Description’ that has more information or related terms specific to a product (including Subscription Offers or Software), service, solution or buying program (e.g. enterprise agreements), available at the Product Specific Terms webpage and the Service Descriptions webpage.

Personal Data	Any information about, or relating to, an identifiable individual that Cisco processes as a Processor for You under the Agreement.
Processor	Shall have the same meaning ascribed to “processor” under the GDPR and other equivalent terms under other Data Protection Laws (e.g.: “Service Provider” as defined under the CCPA), as applicable.
Software	Cisco-branded computer programs, including upgrades and firmware.
Subscription Offer	A Cisco Offer provided on a term, or subscription, basis under the Agreement.
Supplier	A third-party service provider that Cisco engages to process Your Data in connection with Cisco’s provisioning of the Cisco Offers.
You, Your	The individual or legal entity acquiring access to Cisco Offers.
Your Data	Customer Content and Personal Data.



Software License Portability Policy

Purpose

This document sets forth Cisco's policy regarding an authorized licensee's ("Licensee") reassignment of Cisco license entitlements between two (2) devices, either physical or virtual, owned or leased by Licensee and acquired from a Cisco-approved source ("Port" or "Porting"). Licensee's use of the reassigned Cisco software will be governed by the Cisco End User License Agreement ("EULA") and applicable supplemental terms in effect at the time of Porting. Cisco's software licenses are available at www.cisco.com/go/softwareterms.

Policy

A Licensee may Port software license entitlements as set forth below, unless otherwise provided in any supplemental terms. In all cases where feasible, Licensee must deactivate the software on the old device simultaneously with reassignment to the new device.

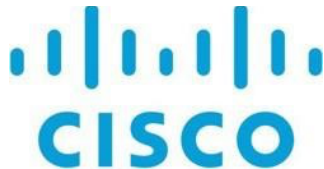
1. **Unassigned Entitlement:** Software license entitlements not assigned to a specific device (including nonCisco devices) may be Ported without restriction.
2. **Device-Specific Subscription Software** may be Ported to any Cisco device within the same technology family (eg security to security; collaboration to collaboration). Any credit due to Licensee for the ported Software subscription will be applied to the amount due for the new subscription.
3. **Device-Specific Perpetual Software:** Licensee may Port:
 - a. Software license entitlements for features from a Cisco device that is supported by active hardware maintenance (eg SmartNet Total Care) to another Cisco device with the same model number (eg as replacement for a defective device); and
 - b. Software license entitlements that expressly include the right to Port in supplemental terms and are supported by Cisco Software Support can be Ported to another device model number, in accordance with applicable portability tiers found at <http://www.cisco.com/c/en/us/products/collateral/software/onesoftware/tiering-guide-cisco-one.html>. For Software purchased as a Suite (eg Cisco ONE Software), Individual components of a Suite are not portable individually.

Definitions

All capitalized terms not defined in this Policy have the same meaning as in the EULA. For purposes of this Policy, the following definitions apply:

1. **"Device-Specific"** means a license entitlement assigned to one particular device (eg IP Base on Catalyst 3650 switch).
2. **"Perpetual Software"** means the Software for which Cisco gives licensee the right to use for an indefinite period of time, as long as such use is in compliance with the terms of the license agreement.

3. **"Subscription Software"** means Software for which Cisco gives licensee the right to use (including to software support services) for a fixed period of time.
4. **"Suite"** means a bundle of related products, features or capabilities sold as a single PID or meter that delivers and specific outcome or addresses a specific use case.



Software License Transfer and Re-Use Policy

1. Purpose

This document sets forth Cisco's policy regarding the transfer and/or re-use of Cisco Software licenses (the **"Policy"**). Transferee's use of Cisco Software is governed by the then-current Cisco End User License Agreement (**"EULA"**) or General Terms, as the case may be, available at www.cisco.com/go/softwareterms.

2. Definitions

All capitalized terms not defined in this Policy have the same meaning as in the EULA. For purposes of this Policy, the following definitions apply:

"Authorized Transfer" means the valid licensee (**"Transferor"**) conveys or assigns the Software license to another entity (**"Transferee"**) after (1) Cisco approves the Software Transfer Request Form referenced herein and (2) licensee pays any applicable license fees (including all outstanding license fees invoiced and paid periodically) or any other conditions required by Cisco.

"Hardware" means Cisco-branded equipment or devices listed on the then-current Cisco global price list (GPL).

"Product" means Cisco-branded Hardware and/or Software.

3. Transfer Policy

Software is not transferable unless (A) applicable law requires it, (B) the applicable license terms expressly permit it, or (C) the transfer is an Authorized Transfer. Cisco may require the Transferee to pay service inspection or reinstatement fees in accordance with [Cisco policies](#) before any transfer.

Upon completion of an Authorized Transfer and unless otherwise provided herein, the Transferor's Software license is automatically terminated. Cisco may withhold consent to any transfer not conforming to this Policy.

The license fee will be equal to the fee for a new individual Software license as specified in the then-current GPL applicable to the Cisco entity in the territory where the Transferee is located. For Software where there is no separate license fee specified in the applicable GPL at the time of transfer, such transfer will be subject to payment of Cisco's then-current applicable software relicensing fee and in accordance with [Cisco's standard terms and conditions of sale](#).

In all cases, (a) Transferor is responsible for ensuring that payment of applicable licenses fees is made and (b) Transferee is not an authorized licensee until Cisco receives payment of the applicable license fee and Transferee's acceptance of the applicable license terms.

4. Exceptions to Transfer

Except as otherwise stated in this Policy or the applicable license terms or other written agreement with Cisco, the following exceptions allow for the transfer of Software by a Transferor without payment of the license fee, provided that the Conditions of Transfer in Section 5 are met.

4.1 Affiliate: A Transferor may transfer its entire right to use Software to its Affiliate. An Affiliate means (a) another entity where more than 50% of its voting power is owned or controlled by the Transferor; (b) the Affiliate owns

or controls more than 50% of the original licensee's voting power; or (c) the same entity owns or controls more than 50% of the voting power of the original licensee and the Affiliate.

4.2 Merger, Acquisition or Divestiture: In the event the Transferor is wholly acquired or merges its business with another entity or sells all or substantially all of its capital stock, or all or substantially all of the assets of that portion of its business to which the applicable Software licenses pertain, Transferor may transfer its right to use the Software to the acquiring or divested entity.

4.3 Financed Software: No leasing company or other financing entity (each, a "**Financing Party**") has any rights under any Software license it may lease to, or finance for, any Cisco authorized reseller or end user. Software license rights and obligations are only between Cisco, as licensor, and the end user identified in Cisco's records, as licensee. If, during or at the end of the term of any lease or other financing of Products consisting of Hardware, the Customer purchases such Hardware (whether pursuant to the terms of a purchase option or otherwise), then the license to any Software embedded in, or bundled with, such Hardware will continue in favor of such Customer on and subject to the terms of the original Software license without any need for a new Software license or the payment of a new license fee. If, however, the Financing Party takes possession or control of any Products consisting of Hardware as a result of any event of default under any lease or financing agreement, the Financing Party may transfer (or cause the transfer of) such Hardware, together with any embedded or bundled Software, to a new lessee or Transferee for the remainder of the license term subject to compliance with this Policy, including the Conditions of Transfer and the payment of the applicable license fee.

4.4 Managed Network Services ("MNS"): A "**Managed Network Service**" is defined as a managed service provider's provision of voice, video, or data network services to an identified end user where the managed service provider is the original licensee and the software is located either in the managed service provider's data center or on the end user's premises.

(A) Original End User: The managed service provider ("**Licensee**" in this Section 4) may transfer the license to the original end user without payment of a license fee if (a) the original end user was entitled to receive MNS pursuant to an MNS agreement with the Licensee, and (b) the Licensee used the Software for a minimum of twelve months prior to the transfer request to provide the original end user MNS. Cisco will issue a license to the original end user granting the right to use the Software once a transfer form is submitted and signed by all relevant parties.

(B) Subsequent MSP: If upon expiration or termination of an MNS agreement, the original end user subsequently contracts with a different managed services provider for the same or equivalent MNS, Licensee may transfer the license to the new managed service provider solely to use the Software to provide the original end user MNS without payment of a license fee.

All other Software license transfers are expressly prohibited, without payment of a new license fee.

4.5 U.S. Government Prime Contractors: For purpose of this exception, US Government Prime Contractors ("**Contractors**") are entities that enter into contracts directly with the U.S. Government through a mutually binding prime contract that obligates the Contractor to furnish the supplies or services and the government to pay for them; and (a) the supplies or services includes use of Software located either in the Contractor's data center or at

the government's premises, and (b) the license to use the Software is held by the Contractor. If the contract between the Contractor and the government end user for whom the Software was first used as part of the Prime Contract ("**Government End User**") either expires or terminates and the Government End User subsequently contracts with a different Contractor for the same services (i.e. follow-on contract), then the license may be transferred subject to the license terms then in effect to the new Contractor, without payment of a license fee, provided, however, that both of the following conditions are met:

- (A) The Software must actually have been used by Contractor solely on behalf of the Government End User and will be deployed and used by new Contractor solely for the benefit of the Government End User;
- (B) The Software must be used only for Government End User's internal use; and,
- (C) Such transfer is a requirement of the Government End User in the follow-on contract.

If the Contractor sells or otherwise transfers the Software without meeting the above conditions, then a new license fee is due.

- 4.6 Outsourcing by Original End User Licensee: If the original end user ("**Licensee**" in this Section 6) desires to outsource the operation, support and/or maintenance of its network to a third party outsourcing company ("**Outsourcer**"), and, as part of the outsourcing arrangement, Licensee desires to transfer its Software licenses to the Outsourcer, it may do so without payment of a new license fee so long as the Software licenses are at all times used for the sole benefit of the Licensee. If Licensee's outsourcing relationship with the Outsourcer terminates or expires, Outsourcer's right to use the software terminates and Outsourcer may transfer the software licenses back to Licensee without payment of a new license fee. Such subsequent transfer is also subject to the Conditions of Transfer below.
- 4.7 Transfers within Europe (consisting of the European Union, Switzerland, Norway, Iceland, and Liechtenstein): An end user located in Europe can transfer Software to another end user Transferee located in Europe without payment of a new license fee, as long as the Software: (1) was originally introduced into Europe by Cisco or Cisco authorized reseller and has not been modified; (2) is used solely for Transferee's internal business purposes; and (3) was originally licensed to the Transferor by Cisco on a perpetual basis and subject to a valid license agreement.

5. Conditions of Transfer

Transfers will only be allowed under the following conditions:

- 5.1 Neither party involved in the transfer is in breach of any agreements with Cisco and/or governing the use of the Software.
- 5.2 The parties involved in the transfer provide written notice to Cisco of any transfer permitted hereunder, indicating that the Transferee agrees to (i) pay any applicable license fee; (ii) assume all obligations of the Transferor; and (iii) use of the Software will be in accordance with the terms of Cisco's then-current license terms for the Software.
- 5.3 The Transferor transfers the Software license in accordance with the original license entitlement, including but not limited to any applicable license metric, duration, and quantity.
- 5.4 The Transferor destroys all copies of the Software (other than the Transferee's copy) in its possession at the time of transfer, and, at Cisco's request, provides written notice to Cisco certifying such destruction and agreeing that its license to use the Software has terminated immediately upon such transfer.
- 5.5 Both authorized parties to the transfer complete and submit the [Software License Transfer Request Form](#) and comply with its requirements.

6. Re-Use Policy

- 6.1 Except as stated below or as otherwise stated in any applicable license terms, where a managed service provider ("**Provider**") desires to re-use Software for a new end user after its agreement with the current end user ceases, Cisco will allow such re-use in accordance with the original license entitlement and without payment of a new license fee, but only if and for as long as all of the following conditions are met: (a) the new end user at all times

continues receiving MNS services from the Provider, (b) the Provider at all times is the Licensee of the Software when providing its services to end users. In addition, for all Cisco One software and perpetual application software, Provider must either maintain an active software maintenance contract (e.g., SWSS), without interruption, or have an active subscription inclusive of annual software maintenance. Service inspection or reinstatement fees may apply in accordance with Cisco policies.

- 6.2 The following Software cannot be re-used without payment of a new license fee: Cisco Unified Workspace Licensing, User Connect Licensing and Contact Center Enterprise.

7. Questions?

Any questions or comments regarding the Transfer Policy should be sent to swtransfer@cisco.com.



Cisco Systems Inc.

Products Supplemental Terms

In this document

- Supplemental Terms – HaaS Terms and Conditions
- Supplemental Terms – Software Innovation Access (SIA)
- End-of-Life Policy
- Cisco Non-Entitlement Policy (External) Version 2.0
- Cisco Limited Hardware Warranty Terms
- Cisco 90-Day Limited Software Warranty



Website references

Throughout the Cisco terms, references to external websites will instead point to attachments included in this package. Links and webpage references in the left column shall mean the document (and section) in the right column.

<i>Link / Reference</i>	<i>Document / Section</i>
Warranties Product Warranties https://www.cisco.com/go/warranty	General Terms & Appendices, Warranty section
Cisco General Terms webpage Software General Terms	General Terms & Appendices,
Data Protection Agreement	General Terms & Appendices, Data Protection Agreement section
Information Security Exhibit	General Terms & Appendices, Information Security Exhibit section
Customer Content – Data Brief webpage	General Terms & Appendices, Customer Content: Data Brief section
Personal Data – Data Brief	General Terms & Appendices, Personal Data: Data Brief section
Systems Information – Data Brief	General Terms & Appendices, Systems Information: Data Brief section
Cisco Software Transfer and Re-licensing Policy http://network.cisco.com/en/US/prod/cisco_software_transfer_relicensing_policy.html .	General Terms & Appendices, Software Transfer and Re-licensing Policy section
Software Portability Policy Software License Portability Policy https://www.cisco.com/go/softwareterms https://network.cisco.com/c/en/us/products/end-user-license-agreement.html	General Terms & Appendices, Software License Portability Policy section General Terms & Appendices Appendix - Offer Descriptions - Products
Cisco RMA Policy for Warrant and Hardware Support Contract Returns	General Terms & Appendices, RMA section
Offer Descriptions Product Specific Terms Product Descriptions Product Offer Descriptions	Follow to website via URL in document
Offer Descriptions Service Specific Terms Service Descriptions Service Offer Descriptions Software Support Service Solution Support	Follow to website via URL in document



Supplemental Terms

HaaS Terms and Conditions

These HaaS Terms and Conditions (the “HaaS Terms”) are Supplemental Terms that form part of the [General Terms](#) or similar terms existing between You and Cisco (including the End User License Agreement) (the “Agreement”). Capitalized Terms, unless defined in this document, have the meaning in the General Terms.

1. Summary

These HaaS Terms set out specific terms that apply to Your access to and use of HaaS (defined below) provided as part of Subscription Offers. The inclusion of HaaS in a Subscription Offer grants You the right to use HaaS for the Use Term by paying the applicable fees.

2. Shipping

2.1 Delivery. The Approved Source will deliver HaaS to the location indicated in the Order. Cisco is not responsible for the installation, maintenance, or repair of HaaS except as expressly stated in the Offer Description or as a separately purchased service.

2.2 Return. You must ensure all HaaS is Returned by the last day of Your Use Term. If You do not, Your Use Term will continue monthly until Cisco either (a) receives the Returned HaaS; or (b) receives payment from You equal to the fair market value of the unreturned HaaS. Cisco’s acceptance of the non-return fee neither transfers title of HaaS to You nor serves as a buy-out fee. Returns are subject to section 3.4 (Risk of Loss) below.

3. Installation, Operation, and Care

3.1 Installation and Use. You will install HaaS according to Cisco’s instructions and use it in conformance with the Offer Description and the Documentation. You will keep HaaS in good working order (reasonable wear and tear excepted) until it is Returned to Cisco. You will keep HaaS in a location that meets the environmental requirements (if any) specified in the relevant Documentation.

3.2 Changes. You may not make alterations or additions to HaaS except where they are (a) required by law; (b) recommended by Cisco in its Documentation (e.g., installing bug fixes); (c) a configurable element of HaaS; or (d) approved in advance by Cisco in writing. Any alterations or additions must be readily removable without damage to HaaS.

3.3 Location. You are not authorized to export HaaS or to move any HaaS outside the country specified in the Order. You may move HaaS within the country specified in the Order, if: (a) You send written notice to Cisco at least 30 days before the move; and (b) for SKUs that include multiple devices in a bundle (as opposed to individual SKUs for each device), all the bundled HaaS comprising the SKU are moved together to one new site. You are responsible for any additional taxes or fees imposed on Your move and use of the HaaS in another location.

3.4 Risk of Loss. You bear the entire risk of loss, theft, or damage to HaaS from the time You receive HaaS until Returned to Cisco. You will notify Cisco in writing promptly if You become aware that HaaS has been lost, stolen, or damaged or has its functionality impaired due to corruption of software, firmware, or other causes.

3.5 Insurance. You will maintain levels of insurance sufficient to fully cover HaaS. Upon request, You will deliver to Cisco a certificate of insurance showing compliance with this requirement.

3.6 Data. You are responsible for backing up Customer Content (including data, configurations, and programs) on HaaS and for deleting it all before Return. Cisco will delete all Data (regardless of the type) from HaaS when Returned. Cisco will have no liability to You for any Data on HaaS upon return to Cisco. This includes Data that would otherwise be considered Confidential Information.

3.7 Prohibited Actions. You will not sell, assign, or lease, or outsource use of any HaaS unless it is expressly allowed by the Offer Description. You will not permit any security interest, lien, or encumbrance to attach to HaaS.

3.8 Substitutions. Cisco may replace, substitute, or update HaaS if such changes do not materially and adversely affect its functionality or performance.

4. Definitions

“HaaS” means any Cisco-branded device obtained through an Approved Source and made available for Your use, where Cisco or its designee retain title to the device during Your Use Term. HaaS is provided as part of a subscription- or service-based Subscription Offer as described in the applicable Offer Description.



Supplemental Terms

Software Innovation Access (SIA)

These Supplemental Terms form part of the [General Terms](#) or similar terms existing between You and Cisco (e.g., the End User License Agreement) (the "Agreement"). Capitalized terms, unless defined in this document, have the meaning in the Agreement.

1. Summary

A Cisco Software Innovation Access ("SIA") subscription provides access to the latest generally available Feature Releases (as defined below) of Your applicable Cisco Order during the SIA subscription term set out in Your SIA Order ("SIA Subscription Term"). A SIA subscription is only available for certain Cisco Orders licensed on a perpetual basis.

2. Supplemental Terms

2.1 Requirements. For any Cisco Order covered by a SIA subscription, You must have: (a) SIA subscription coverage for your entire deployment of the applicable Cisco Order; (b) Cisco software support and maintenance contract coverage for your entire deployment of the applicable Cisco Order for the duration of the SIA Subscription Term, including any renewals; and (c) corresponding licenses (e.g., Right-to-Use or RTU licenses) to Your entire deployment of the Cisco Order licensed on a perpetual basis.

2.2 Feature Releases. Cisco will provide You with access to Major Releases and Minor Releases of the applicable Cisco Order, if and when available during the SIA Subscription Term ("Feature Releases"). Feature Releases do not include Maintenance Releases. Your use of a Feature Release is limited to Your Use Rights to the applicable Cisco Order. A SIA subscription does not include custom feature development. Features and functionality of a Feature Release are set out in its Documentation. You will not have access to new Feature Releases following the end of sale date of the applicable Cisco Order. You may not download or activate a Feature Release following expiration or termination of Your SIA subscription. Even though Your deployment of a Cisco Order is licensed on a perpetual basis, SIA is ordered as a subscription for the specific SIA Subscription Term and only for the applicable licenses of the Cisco Order that you have purchased as set out in Your Order for the Cisco Order.

2.3 Additional Responsibilities. You must: (a) download and use only the Feature Releases that You are entitled to use based on Your Order; (b) cease using the previous releases of the Cisco Order after successfully transitioning to a new Feature Release; (c) not transfer previous releases of the Cisco Order; and (d) register and report license usage for the Cisco Order via Cisco Smart Software Manager, with periodic license usage reporting enabled, if available for the Cisco Order. For a more detailed overview on Cisco Smart Licensing, go to cisco.com/go/licensingguide.

2.4 Expiration & Reinstatement. At the expiration of the SIA Subscription Term, You may continue to use the last licensed Feature Release installed when the SIA Subscription Term expired, in accordance with the General Terms and any applicable Order Description. If You wish to reinstate an available SIA subscription on the Cisco

Order after expiration of the SIA Subscription Term, You must pay: (a) the amount You would have paid for the SIA subscription for the Cisco Order between expiration and the date of reinstatement ("Lapsed Period Fee"); (b) reserved; and (c) the then-current fee for the new SIA Subscription Term.

2.5 Definitions

<i>Term</i>	<i>Meaning</i>
Maintenance Release	An incremental Software release that provides maintenance fixes and may provide additional Software functions. Cisco designates Maintenance Releases as a change in the digits to the right of the tenths digit or of the hundredths digit of the Software version number [x.x.(x) or x.x.x.(x)].
Major Release	A release of Software that provides additional Software functions. Cisco designates Major Releases as a change in the ones digit of the Software version number [(x).x.x].
Minor Release	An incremental release of Software that provides maintenance fixes and additional Software functions. Cisco designates Minor releases as a change in the tenths digit of the Software version number [x.(x).x].

End-of-Life Policy

Purpose

All products reach the end of their life cycle for several reasons, including market demands, technology innovation and development-driven changes, or product maturity and replacement with functionally richer technology. Even so, Cisco also recognizes that end-of-life (EOL) milestones often prompt companies to review the impact to the Cisco products, services, or subscriptions in their networks. With that in mind, we have set out below Cisco's End of Life milestones to help manage EOL transitions and to explain the role that Cisco can play in helping to migrate to alternative Cisco technology.

Scope

Cisco's End of Life Policy ("Policy") applies to all Cisco hardware, software, cloud services and service offers (collectively "Products") that have their own unique product part number or product identifier ("PID").* Versions or releases of a Product that do not have a unique PID are not subject to this Policy.

This Policy covers all new EOL notifications made in all theaters on or after September 29th 2022. It does not apply to a Cisco Product that is already subject to an EOL notification as of September 29th 2022.

Policy

End of Life Milestones:

- External notification of end of sale is typically six (6) months before the End of Sale ("EOS") date, which is the date after which you can no longer purchase the relevant Cisco Product. Such notice will appear on cisco.com at <http://www.cisco.com/c/en/us/products/eos-eol-listing.html>. Please visit this site regularly as it contains useful information regarding Cisco's end-of-life program. Sign up to receive notifications at the [Cisco Notification Service](#).
- No subscriptions (including renewals) with a term extending beyond Last Day of Support ("LDOS") will be sold after the EOL Notification Date."
- The Last customer ship date for hardware is three (3) months after the hardware EOS date.

Cisco will provide the following to customers with active support contracts or subscriptions (including cloud services): One (1) year of routine failure analysis for hardware from the EOS date.

- One (1) year of bug Fixes, maintenance releases, workarounds or patches for critical bugs from the EOS date, when reported to TAC. After the 1st year, Cisco will provide bug Fixes, workarounds and/or patches, where available, for (i) two (2) years for OS software, and (ii) one (1) year for application software. Customers may be required to install a newer software version to receive the above software support.
- Three (3) years of TAC support for OS software from the software EOS date, except for the final release of the OS software running on EOS hardware as noted below.
- Two (2) years of TAC support for application software from the EOS date.
- TAC support from the EOS date until the end of the term for subscription software and cloud services.
- Five (5) years of TAC support for hardware from the EOS date. TAC support for the final release of OS software running on the EOS hardware will be coterminous with the hardware LDOS, regardless of the OS software EOS date.
- Five (5) years of replacement parts for hardware from the EOS date, in accordance with Cisco's Return Materials Authorization (RMA) process.

Customers may:

- Add a new support contract to hardware (including OS software) and application software for up to one (1) year from the EOS date, provided the contract end date does not exceed LDOS.

- Renew support contracts for hardware (including, OS software) and application software, provided the contract end date does not exceed LDOS.
- Renew or add on to an existing software subscription or cloud service on or after the EOS date, provided the new subscription end date does not exceed the last date the subscription or cloud service is available as determined by Cisco.

EOL Milestone Table

EOL Milestone Table

Event or Support Activity	- 6 Months	Day 0	3 Months	1 Year	2 Years	3 Years	4 Years	5 Years
End of Life Notification Date	◆	End of Sale date						
End of Sale Notice Period								
Last Customer Ship Period								
Hardware (with Service)								
Cisco TAC support								
Add or attach new service contracts (purchase)								
Renew service contracts								
Last Date of Support								◆
OS Software								
Cisco TAC support								
Software maintenance releases								
Last Date of Support							◆	
Application Software (with Service)								
Cisco TAC support								
Software maintenance releases								
Last Date of Support						◆		
Software Subscriptions	◆	◆						
End of Sale subscription term greater than LDOS								
End of auto-renew for new subscriptions								
Existing subscriptions								
Renew (manual / auto-renew)								
Changes (modify - delete/replace)								
Changes add-on (modify - add quantity)								
Last Date of Support								

Table 1. Standard Guideline for End-of-Life Milestones

As defined in the external announcement

End of the subscription term

As defined in the external announcement

As per the term of the subscription

Definitions

For purposes of this policy, the following definitions apply:

- **End of Life (EOL):** A process that guides the final business operations associated with the Cisco Product life cycle. The end-of-life process consists of a series of technical and business milestones and activities that, once completed, make a Product obsolete. Once obsolete, the Product is not sold, improved, maintained, or supported.
- **End of Sale date (EOS):** The Product is no longer ordered for sale after this date. This is also the last date to order the Product through Cisco point-of-sale mechanisms. The EOS date is documented in the EOL notification.
- **EOL Notification Date:** The date on which the end of sale and the end-of-life milestones for a Product is communicated to the public
- **Last Date of Support (LDOS):** The last date to receive support as entitled by active service contracts for covered Cisco hardware and software. After this date, support is no longer available

*Meraki PIDs will be subject to the [Meraki Product End-of-Life \(EOL\) Policy](#).

**[Cisco Networking Subscriptions](#) (including renewals) with a term extending beyond Last Day of Support may be sold after the EOL Notification Date. Please note that the continued sale and application of these subscriptions to LDOS hardware will not extend the support (hardware, software or TAC) of such hardware.

Cisco Non-Entitlement Policy (External) Version 2.0

1. General Conditions

You are solely responsible for maintaining an inventory of Products and Software ("Installed Base") necessary to establish entitlement to Services. Cisco may assist You with maintaining an up-to-date Installed Base inventory by making available My Cisco Entitlements self-help tools.

1.1 Services or Warranty entitlements that are not expressly set forth in the applicable Service Description or Warranty document are not covered under such Services Description or Warranty entitlement including, without limitation, the following:

- (a) Support or replacement of a Product that is altered, modified, mishandled, destroyed, or damaged by one or more of the following:
 - (1) natural causes;
 - (2) environmental failures;
 - (3) Your failure to take any required actions;
 - (4) a negligent or willful act or omission by You or use by You other than as specified in the applicable Cisco-supplied Documentation;
 - (5) intentional permanent cosmetic alterations;
 - (6) an act or omission of a third party.
- (b) Support or replacement of Product that was inoperable prior to purchase of a maintenance contract with Cisco.
- (c) Support of Product beyond the identified Last Day of Support ("LDoS") date, regardless of whether such Product has been included in any chassis-based service pricing.
- (d) Services for Products:
 - (1) for which a valid maintenance contract is not in place; or,
 - (2) Services or Warranty coverage for Products with an expired Warranty coverage date and no active Service contract.
- (e) Services for a Product that Cisco determines is Non-Genuine Product. Any warranty support or Services for a Product determined to be a Non-Genuine Product is void. Cisco reserves the right to immediately terminate any associated support service contract or Warranty, and any replacement parts or other materials made available in connection with that Non-Genuine Product must be returned to Cisco.
- (f) Services and Warranty are only provided for generally available Products and Software releases/versions.
- (g) Services or software to resolve Software or Hardware problems resulting from third-party product(s) or causes beyond Cisco's control.
- (h) Furnishing of supplies, accessories, or the replacement of expendable parts (e.g., batteries, cables, blower assemblies, power cords, and/or rack mounting).
- (i) Cisco uses solid-state drives from various vendors. All solid-state drives are subject to physical write limits and have varying maximum usage limitation specifications set by the manufacturer. Cisco will not replace any solid-state drives that have exceeded any maximum usage specifications set by Cisco or the manufacturer, as determined solely by Cisco.

(j) Hardware replacement in quantities greater than three (3) FRUs, including those replacements due to pervasive issues documented in an engineering change notice or field alert unless End User has troubleshoot each failed Hardware down to the FRU level.

(k) Any Hardware or Third-Party Product upgrade required to run new or updated Software.

(l) Any customization of, or labor to install, Software and Hardware (including installation of updates).

(m) Erasure or removal of any of Your or third-party data on Products (or parts thereof) returned, repaired, or otherwise handled by Cisco.

(n) Services for Product where service contract was purchased from a source other than Cisco or its Authorized Channel.

(o) Services for Product where Cisco Software license(s) deposited on Smart Licensing platform associated with the Product were purchased, modified, or otherwise used in violation of the applicable terms. Cisco reserves its right to:

(1) invoice the party for the authorized Cisco Software license; and,

(2) pursue other available remedies, including termination of Services, as well as Cisco user profiles and access rights.

2. Deployment and Delivery

Cisco provides support for our installed products in commercial or governmental locations not requiring specialized access equipment and meeting all local safety regulations. Products are delivered to the normal postal delivery address or freight dock by regulated delivery services. Cisco does not provide:

2.1 Services for Products that are (a) installed outdoors or (b) installed indoors but require specialized equipment to perform such Service. Cisco will not supply specialized access equipment and will not perform Service until You provide access that meets applicable local labor laws and workplace safety rules for Cisco employees and contractors.

2.2 Services performed at domestic residences.

2.3 Any expenses incurred to visit End User's location, except at Cisco discretion during escalation of problem resolution by Cisco.

2.4 Electrical or site work external to the Products. This also excludes any installation staff, such as a licensed electrician for direct interconnect of power, or installation work not covered by a specific installation contract SOW.

3. Software

Cisco provides support for selected software products and Third-Party solution components. Cisco does not provide:

3.1 Services on non-authorized software.

3.2 Warranty or Service coverage for Product or Software support, including updates and bug fixes for which (a) a valid license for the Product is not in place or (b) Product which was purchased from a source other than Cisco or its Authorized Channel. Cisco reserves the right to: (1) suspend support associated with such Products until such time as any applicable inspection is conducted and any applicable relicensing fees are paid for such Products or (2) terminate the support service contract and/or Warranty.

- 3.3 Support for any Software release that has reached LDoS.
- 3.4 Open Source, community-supported project software.

4. Cloud and Remote Software Services

<Reserved>

5. Non-Cisco Hardware and Software

Cisco may, as part of authorized Solutions, support use of authorized Third-Party components and SW products. Those items shall be specified in the individual Solution Service Description. Cisco does not support:

5.1 Third-Party Components. The Cisco guideline for support and warranty services for the use of non-authorized third-party memory, cables, interface modules, filters, or other non-Cisco authorized components is as follows:

(a) When You report a product fault or defect and Cisco believes the fault or defect can be traced to the use of third-party memory products, cables, interface components, filters, or other non-Cisco authorized components by You or a reseller, then, at Cisco's discretion, Cisco may withhold support under warranty or a Cisco support program. If Cisco concludes that the fault or defect is not attributable to the use of third-party memory, cables, interfaces, filters, or other non-Cisco authorized components installed by You or a reseller, Cisco will continue to provide support for the affected product under warranty or covered by a Cisco support program.

(b) Cisco also reserves the right to charge You for services provided to You when Cisco determines, after having provided such services, that the root cause of the defective product was caused by a non-supported third-party vendor supplied product.

5.2 Third party repairs or repair components are also grounds for Cisco to cancel service or warranty support. Cisco may pursue recovery of parts provided to replace product later found to have previous third-party repairs or components.

6. Non-Genuine, Destroyed, or Stolen Product

This section sets forth the invalidity of warranty and service support for any Destroyed, Stolen, or Scrapped Product. This policy is intended to support and be consistent with other relevant Cisco policies, such as those regarding Cisco trademarks and copyright materials, Software Licensing, Non-Genuine Products, programs that permit Cisco's Authorized Channel to sell legitimate and genuine Products and Services, and any other Cisco policies referenced in this policy.

6.1 Warranties. Cisco does not offer any kind of warranty support for Destroyed, Stolen, or Scrapped Products. None of Cisco's written warranties (as set forth at <https://network.cisco.com/c/en/us/products/warranty-listing.html> or elsewhere) applies to any Destroyed, Stolen, or Scrapped Products.

6.2 Services. Cisco does not offer for sale or otherwise any Services for Destroyed, Stolen, or Scrapped Products. None of Cisco's service offerings applies to any Destroyed, Stolen, or Scrapped Products.

6.3 All service contracts and/or Hardware or Software warranty obligations pertaining to Destroyed, Stolen, or Scrapped Products are void. Upon Cisco's discovery and verification of products as Destroyed, Stolen, or Scrapped Products, Cisco will immediately terminate all associated Services and/or

warranty support for such Destroyed, Stolen, or Scrapped Products, and may take other available actions. You are not entitled to a refund for associated termination of support for Destroyed, Stolen, or Scrapped Products.

6.4 Refurbished Equipment. Cisco does not offer Services, or authorize or endorse any third party, to refurbish any Destroyed, Stolen, or Scrapped Products. Cisco's Authorized Refurbished Equipment Program (located at [https://network.cisco.com/c/en/us/buy/cisco-capital-](https://network.cisco.com/c/en/us/buy/cisco-capital-finance/refresh/overview.html)

[finance/refresh/overview.html](https://network.cisco.com/c/en/us/products/network-sw-relicensing-program.html#~policy#~using)) and related Software licensing (located at <https://network.cisco.com/c/en/us/products/network-sw-relicensing-program.html#~policy#~using>) do not apply to any Destroyed, Stolen, or Scrapped Products. Inspections. Cisco does not offer, authorize, or endorse any used equipment inspection or recertification for Destroyed, Stolen, or Scrapped Products.

6.5 Return Material Authorization. Cisco does not accept Destroyed, Stolen, or Scrapped Products as a part of Cisco's RMA process for Advance Replacements. Destroyed, Stolen, or Scrapped Products sent to Cisco either directly or via a Cisco-Authorized Channel will not qualify as meeting Cisco's RMA requirements.

6.6 Any Cisco product that has been identified as a Destroyed, Stolen, or Scrapped Product (per serial number) will be appropriately identified in Cisco's databases as ineligible for any kind of warranty or service support.

6.7 Any otherwise valid warranty support or Services for a Cisco product that becomes subject to destruction, reported theft, or scrapping will immediately become void and terminate upon such destruction.

6.8 Cisco does not have any obligation or liability for Destroyed, Stolen, or Scrapped Products.

6.9 If, per Cisco's Advance Replacement Services or Warranty support, You receive a replacement product from Cisco and then improperly return to Cisco a Destroyed, Stolen, or Scrapped Product (instead of the actual matching serial number defective Product for which the Advance Replacement product was provided), Cisco retains the right to invoice You for a genuine Cisco replacement product, and may take other actions, including, termination of the Your support contract and/or pursue other available actions or otherwise fail to return the specified RMA Product.

6.10 Cisco encourages the removal of all Destroyed, Stolen, or Scrapped Products from Your Network in order to eliminate or reduce risks associated with keeping such Destroyed, Stolen, or Scrapped Products in the Network.

6.11 Destroyed, Stolen, or Scrapped Products are ineligible for Cisco Software licensing agreements or any other assignments of Cisco Operating License rights.

7. Non-Entitlement to Cisco Warranty and Service Support of Unauthorized Products and Illegally Imported Products

7.1 Services and Warranty. Illegally Imported Products and Unauthorized Products are not eligible for Cisco warranties. Illegally Imported Products are ineligible for support services. Unauthorized products may only become eligible for support services following a successful physical inspection and appropriate proof to Cisco showing that any applicable appropriate Software license fees have been paid for the said Unauthorized Products (or that payment is made for such licenses if no prior payment has been made) by or on behalf of the End User who will be using the Unauthorized Products in question. Fees, such as those for reinstatement of services, may apply.

7.2 Refurbished Equipment. Cisco does not authorize or endorse any third party to refurbish Unauthorized Products. However, Cisco does offer refurbished products for sale through the Cisco

Authorized Refurbished Equipment Program. Information about the program is available at: <https://network.cisco.com/c/en/us/buy/cisco-capital-finance/refresh/overview.html> Information about Cisco's Software License Transfer and Re-Use Policy is available at: http://network.cisco.com/en/US/prod/cisco_software_transfer_relicensing_policy.html.

7.3 Inspection Fees. Contact your local Cisco service account representative for more information about Cisco's inspection fees and process.

7.4 Software Support. You may only download, install, and expect support for Software versions and feature sets for which they have purchased a valid license that is current and active. By installing, downloading, accessing, or otherwise using such software updates, You agree to follow the terms of the currently published Cisco General Terms. In most cases, the Software Update will be a maintenance release to software that was previously purchased. Free security software updates do not entitle You to a new software license, additional software feature sets, or major revision upgrades.

7.5 Any Illegally Imported Product is ineligible for any Cisco warranty, service, or software support. Any Unauthorized Product is ineligible for any kind of Cisco warranty. Any Unauthorized Product is ineligible for any service, or software support unless it becomes eligible through inspection, applicable licensing, and/or other applicable processes. Cisco reserves the right to terminate any service contract or deny service coverage on Illegally Imported Products and Unauthorized Product. Cisco reserves the right not to issue any refund associated with termination of service contracts on Illegally Imported and Unauthorized Products.

7.6 Cisco assumes no obligation or liability for Unauthorized Products, except as detailed in service contracts written after such Products have been inspected and appropriate Software licenses have been purchased.

Cisco may:

- (a) invoice You for the genuine Cisco replacement Product; and/or,
 - (b) pursue other available actions, such as termination of the Your support contract
- when You:
- (1) receive a replacement product from Cisco; and,
 - (2) return an ineligible Unauthorized Product instead of the actual defective Cisco product for which the Advance Replacement Product was provided or anything except the specified Product in the RMA.

7.7 Cisco encourages You to check the source and quality of the Products they purchase, in order to reduce risks of purchasing and using Illegally Imported Products and Unauthorized Products in Your Network. Cisco encourages You to check eligibility of Unauthorized Products for Cisco support and the validity of the applicable Software licenses for those Products.

8. Non-Entitlement to Cisco Warranty and Service Support of Non-Genuine Cisco Products

The integrity of a Your Network is of paramount importance. Cisco's ability to properly support Your Network is premised on the basis that the Cisco products and software in such Network comprise genuine products/software that have not been destroyed, stolen, or otherwise constitute scrapped materials. This policy sets forth the invalidity of any warranty and service support for a Non-Genuine Product. This policy is intended to support and be consistent with other relevant Cisco policies, such as those regarding Cisco trademarks and copyright materials, software licensing, destroyed, stolen and scrapped products, channel partner direct and indirect programs that authorize Cisco Channel Partners to sell legitimate and genuine Cisco products and services, and any other Cisco policies referenced in this policy.

8.1 Warranties. Cisco does not provide any kind of warranty support for Non-Genuine Products. None of Cisco's written warranties (as set forth at <https://network.cisco.com/c/en/us/products/warranty-listing.htm> or elsewhere) applies to any Non-Genuine Products.

8.2 Services. Cisco does not offer for sale or otherwise any kind of services for Non-Genuine Products. None of Cisco's service offerings (as set forth on any of Cisco's Price Lists) applies to any Non-Genuine Products.

8.3 All service contracts and/or Hardware or Software warranty obligations pertaining to Non-Genuine Products are void. Upon Cisco's discovery of any Non-Genuine Products, Cisco will immediately terminate all associated services and/or warranty support for such Non-Genuine Product and may pursue other available legal remedies. No refund will apply for terminating all associated services support for Non-Genuine Products.

8.4 Refurbished Equipment. Cisco does not offer services, or authorize or endorse any third party, to refurbish any Non-Genuine Products. Cisco's Authorized Refurbished Equipment Program (found at <https://network.cisco.com/c/en/us/buy/cisco-capital-finance/refresh/overview.html>) and related software licensing (found at <https://network.cisco.com/c/en/us/products/network-sw-relicensing-program.html#~policy#~using>) do not apply to any Non-Genuine Products. Hence, sections (8.1) and (8.2) above are equally applicable to Non-Genuine Products that have been subjected to any type of refurbishment efforts.

8.5 Inspections. Cisco does not offer, authorize, or endorse any kind of used equipment inspection or recertification for Non-Genuine Products.

8.6 Return Material Authorization. Cisco does not accept Non-Genuine Products as a part of Cisco's Return Material Authorization ("RMA") process for Advance replacements. Non-Genuine Products sent to Cisco either directly or via a Cisco-authorized reseller will not qualify as meeting Cisco's RMA requirements and may be subject to destruction.

8.7 Any Hardware or Software that has been identified as a Non-Genuine Product will be appropriately identified in Cisco's databases as ineligible for any kind of warranty or service support.

8.8 Cisco assumes no obligation or liability for Non-Genuine Products.

8.9 If, per Cisco's Advance Replacement services and warranty support, You receive a replacement Product from Cisco and then improperly returns to Cisco a Non-Genuine Product, Cisco retains the right to invoice You for a genuine Cisco replacement Product. Additionally, Cisco may pursue other available actions, including but not limited to termination of Your support contract.

8.10 Cisco encourages the removal of all Non-Genuine Products from Your Network to reduce risks associated with keeping Non-Genuine Products in the Network.

9. Third-Party Repair Sources: Cisco Warranty and Service Support Implications

Cisco Systems® holds ISO 9000 and ISO 14000 certifications and strives to ensure the highest levels of product quality and Your satisfaction. Cisco® contracts with qualified service repair companies worldwide to maintain ISO certifications and provide End User satisfaction. These companies (as subcontractors to Cisco) provide support in connection with Cisco warranty and service contract obligations.

9.1 Cisco employs the authorized repair companies to evaluate, repair, or replace parts or products, including FRUs. An FRU is any component or subassembly of an item, or unit of a product manufactured by Cisco that can be replaced in the field. Example items include chassis, pluggable modules, power supplies, and product-specific printed circuit board assemblies such as line cards.

9.2 Cisco authorized service repair partners receive specialized, ongoing training to competently provide product evaluation, refurbishment, and testing support. Cisco grants these partners access to certified replacement parts, such as the following:

- (a) Engineering Change Order (ECO) processes for latest updates;
- (b) Test plans and procedures developed by Cisco engineers;
- (c) Dynamic burn-in chambers and profiles;
- (d) Fully integrated, automated, and operational test stations in support of the test plan, including all commercial test systems required
- (e) Auto test Scripts, which control the testing process and data gathering;
- (f) Test methodologies such as those specific to a product family and defined by Cisco, which would include tests for structural integrity, functionality, optical parametrics, and live traffic; and,
- (g) A quality assurance program that verifies product functions and reliability without compromising Your needs.

10. Third-Party Repair Sources

10.1 Cisco authorized service repair partners should be distinguished from third-party repair businesses who offer their own brand of repair or other services for Cisco Products. The third-party repair businesses referenced here should also be distinguished from Cisco Authorized Channel partners and resellers per Cisco Channel Partner Program.

- (a) Cisco does not offer or provide any warranty for products that are repaired by such third-party service repair businesses. Unauthorized repair voids the Cisco Warranty Entitlement. End Users who elect to use such third-party repair sources do so at their own risk.
- (b) Cisco does not “certify,” “authorize,” “endorse,” or “recommend” any third-party service repair businesses and cannot validate or otherwise comment upon their competencies, capabilities, or qualifications.
- (c) Cisco does not offer or provide any replacement or spare parts to third-party service repair businesses.
- (d) All Cisco software license grants are to End Users and are non-transferable. See Cisco Software General Terms at <https://network.cisco.com/c/en/us/products/end-user-license-agreement.html>, including the provisions that prohibit the transfer, assignment, or sublicense of the license to any other person, or to use the Software on unauthorized or second-hand Cisco equipment.

10.2 When You report a product fault or defect and Cisco determines that the fault or defect can be traced to the use of a third-party repair business, Cisco retains the right to withhold support under warranty or a Cisco support program, such as Smart Net Total Care® services.

- (a) Cisco reserves the right to charge You for services provided to You when Cisco determines, after having provided such services, that the root cause of the defective product was due to a third-party vendor or a third-party-vendor-supplied product. If Cisco concludes that the fault or defect is not attributable to the use of a third-party repair company, Cisco will continue to provide support for the affected product under warranty or covered by a Cisco support program.
- (b) End Users who choose to install or use third-party components including, but not limited to, memory, cables, or pluggable modules, do so at their own risk.

(c) For more information about Cisco's Limited Warranty, see:
<https://www.cisco.com/c/en/us/products/warranty-listing.html>.

Glossary

1. "Authorized Channel" includes:
 - 1.1 Cisco sales directly to You;
 - 1.2 Cisco sales to Cisco Channel Partners (who sell directly to You, or within the European Economic Area (EEA) also to other Cisco Channel Partners or Distributors); and,
 - 1.3 Cisco Distributors (who sell to Cisco Channel Partners who resell to You, or within the EEA also to other Cisco Channel Partners or Distributors) where the purchasers of such product are within the contractually agreed territories for the Cisco Channel Partner or Distributor in question.
 - 1.4 Note: For Cisco Channel Partners in the EEA, this includes sales to parties within all the EEA.
2. "Cisco Distributors" means Cisco Distributors, Distribution Partners, or Authorized Distributors authorized by Cisco to resell Cisco Equipment in the territory in which the End User is located, as published on the Cisco Distributor Locator, at the following URL:
<https://www.ciscochannelconnect.com/DistiLocator> as updated from time to time by Cisco.
3. "Cisco Channel Partners" means the Cisco Registered, Certified (Gold, Silver, Premier, Select, etc.), and Specialized Partners authorized by Cisco to resell Cisco Equipment in the territory in which the End User is located, as published on the Cisco Partner Locator, at the following URL:
<https://locatr.cloudapps.cisco.com/WWChannels/LOCATR/openBasicSearch.do> , as updated from time to time by Cisco.
4. "Destroyed" means Cisco products that have been determined to have been "destroyed" under any circumstances, and declared as such, including, but not limited to, accident or natural causes (e.g., earthquake, hurricane, fire, flood, or other exposure to adverse environmental conditions) or due to any negligent or wilful or unlawful act or omission to act (including acts of terrorism and/or or exposure to harmful substances, conditions, or materials).
 - 4.1 "Destroyed" can also mean those products that have been identified as "destroyed" by You, authorized Cisco reseller, distributor, or other third party (e.g., insurance carrier for You) that legally takes possession or title to the "destroyed" products, on a Certificate of Destruction that is provided to Cisco.
5. "FRU" means Field Replaceable Unit.
6. "Illegally Imported Product(s)" means new or used Cisco products that are imported into specific country or region without Cisco's consent, in violation of applicable laws and Cisco intellectual property rights.
7. "Non-Genuine" means any Cisco product:
 - 7.1 to which a Cisco Partner logo, Cisco trademark, service mark or any other Cisco mark has been affixed without Cisco's express written consent;
 - 7.2 (ii) that have not been manufactured by Cisco or by a licensed manufacturer of Cisco;
 - 7.3 (iii) are produced with the intent to counterfeit or imitate a genuine Cisco Product, or
 - 7.4 (iv) where any form of copyright notice, trademark, logo, confidentiality notice, serial number or other product ident.

8. "Scrapped" means any Cisco product that has reached the end of its useful life or which, for quality control or other reasons, Cisco designates for disposal by Cisco or a Cisco authorized repair partner.
9. "Stolen" means any Cisco product that You have reported to the appropriate legal authorities as stolen and has likewise notified Cisco, through customer's designated representative(s). Cisco may seek verifying information from You or law enforcement authorities as to the status of the relevant product.
10. "Unauthorized" means new or used Cisco products that are sourced and/or sold outside Cisco's Authorized Channels network

Cisco Limited Hardware Warranty Terms

WARR-90-DAY-LTD-HW

The following are terms applicable to your Hardware.

Your Cisco operating system Software is subject to the General Terms.

1. Duration of Hardware Warranty

1.1 90 Day Limited Warranty

(a) In the event of discontinuance of product manufacture, the term of the hardware warranty will end on the Last Date of Support (LDOS) published in the product End of Life announcement available here.

2. Warranty Replacement Terms

2.1 Standard Advance Replacement (A/R)

(a) Cisco or its service center will use commercially reasonable efforts to ship a replacement part to the customer's address of record within ten (10) Cisco Business Days after issuance of a valid RMA request. Actual delivery times may vary depending on Customer location. Taxes and duties may apply and will be borne by the recipient of the replacement part.

(b) To make a claim for breach of these warranties, promptly notify your Approved Source within any specified warranty period.

3. Warranty Start Date

3.1 Limited Hardware Warranty

(a) Cisco Systems, Inc., or the Cisco Systems, Inc. subsidiary selling the Product ("Cisco") warrants that commencing from the date of Cisco shipment to Customer (or in case of resale by Cisco shipment to a Cisco Approved Source), commencing not more than ninety (90) days after original shipment by Cisco, and continuing for a period of the longer of

(i) ninety (90) days or

(ii) as otherwise set forth in this document as provided at <https://cisco.com/go/warranty>, the Hardware will substantially comply with the Documentation and be free from defects in material and workmanship under normal use.

(b) The date of shipment of a Product by Cisco is set forth on the packaging material in which the Product is shipped.

(c) This limited warranty extends only to the original End User of the Product. Customer's sole and exclusive remedy and the entire liability of Cisco and its suppliers under this limited warranty will be, at Cisco's or its service center's option, shipment of a replacement within the warranty period and according to the replacement process described in the warranty card (or if no warranty card, as described on the Cisco Product Warranties web page <https://www.cisco.com/go/warranty>) or a refund of the purchase price if the Hardware is returned to the party supplying it to Customer, freight and insurance prepaid.

(d) Cisco replacement parts used in Hardware replacement may be new or equivalent to new.

(e) Cisco's warranty obligations are conditioned upon the return of affected Hardware in accordance with Cisco's or its service center's Return Material Authorization (RMA) procedures and in accordance with the Cisco RMA Policy for Warranty and Hardware Support Contract Returns.

3.2 Restrictions: This limited warranty does not apply if the Hardware:

- (a) has not been used according to its Documentation;
- (b) has been altered, except by Cisco or its authorized representative;
- (c) has been subjected to abnormal or improper environmental conditions, accident or negligence, or installation or use inconsistent with Cisco's instructions or the terms on which it is supplied by Cisco;
- (d) is provided on a trial, evaluation, beta or other free-of-charge basis; or,
- (e) has not been provided by an Approved Source.

4. Warranty End Date

4.1 Cisco Systems, Inc., or the Cisco Systems, Inc. subsidiary selling the Product ("Cisco") warrants that the Warranty End Date will be calculated per the formulation in section 3.1 (a) above.

(a) All new Warranty claim requests will end on the Warranty End Date.

(b) All valid Warranty claims received by Cisco or its Approved Source before 5:00 PM Pacific Time, or 5:00 PM Pacific Time if in effect, will be considered valid even if RMA processing has not yet occurred.

(c) Cisco LIFE Warranties will set Warranty End Date to align with the product published LDOS once End Of Sale is announced.

(d) In the event of Cisco Systems, Inc., or the Cisco Systems, Inc. subsidiary selling the Product ("Cisco") announcing an early End of Sale for a product the Warranty will end on the early LDOS date announced in the End Of Sale notice. Final claims date or other migration information shall be published in a Field Notice, Product Bulletin, or both.

5. DISCLAIMER OF WARRANTIES

5.1 Except as provided in Section 3.1 above, and to the extent allowed by law, Cisco makes no express or implied warranties of any kind regarding the Hardware. This disclaimer includes any warranty, condition or other term as to merchantability, merchantable quality, Fitness for purpose or use, course of dealing, usage of trade, or non-infringement. Cisco does not warrant that the Hardware will be secure, uninterrupted or error-free.

5.2 Customers may have legal rights in their country that prohibit or restrict the limitations set out in Sections 3 and 4. These sections apply only to the extent permitted under applicable law.

6. Liability

6.1 Excluded liability. Neither party is liable for:

- (a) indirect, incidental, reliance, consequential, special or exemplary damages; or

(b) loss of actual or anticipated revenue, profit, business, savings, data, goodwill or use, business interruption, damaged data, wasted expenditure or delay in delivery (in all cases, whether direct or indirect).

6.2 Liability cap. Each party's entire liability for all claims relating to this warranty will not exceed the fees paid to Cisco for the Hardware that is the subject of the claim. This cap is cumulative for all claims (not per incident). Nothing in this limited warranty limits or excludes any liability that cannot be limited or excluded under applicable law. The foregoing limitation of liability shall not apply to (1) personal injury or death resulting from Licensor's negligence; (2) for fraud; or (3) for any other matter for which liability cannot be excluded by law.

7. Governing Law and Venue

7.1 These terms, and any disputes arising from them, are subject to the governing law and exclusive jurisdiction and venue listed below, based on Your primary place of business. Each party consents and submits to the exclusive jurisdiction of the courts in the listed venue. These laws apply despite conflicts of laws rules, or the United Nations Convention on Contracts for the International Sale of Goods. Despite the below, either party may seek interim injunctive relief in any court of appropriate jurisdiction regarding any alleged breach of confidentiality obligations or intellectual property or proprietary rights.

(a) If You are a US State, Local and Education Government end user, these terms, and any disputes arising from them, are subject to the laws of the primary jurisdiction in which You are located.

(b) If You are a US Federal Government end user, these terms, and any disputes arising from them, are subject to the Federal laws of the United States.

8. How to Return Parts:

8.1 Return Materials Authorizations

(a) All material returned to Cisco must be accompanied by a Return Material Authorization (RMA) number issued by Cisco to ensure tracking and handling of returned material. The Cisco Returns Portal provides instructions on obtaining an RMA number and returning items to Cisco.

(1) Please note that destination country importation, compliance with US export controls, and customs processes may condition actual delivery times. Advance replacements to and from the European Union will be shipped Delivered Duty Paid (DDP) (Incoterms 2020). All other replacements will be shipped Delivered At Place (DAP) (Incoterms 2020), exclusive of any import duties, taxes and fees, where applicable. All replacements will be shipped using Cisco's preferred carrier, freight prepaid by Cisco.

(2) If you do not have an RMA number, Cisco reserves the right to refuse receipt of returned units.

(b) To Receive a Return Materials Authorization (RMA) Number:

(1) Please contact the Approved Source from whom you purchased the product. Guidance on Product returns is given in the Warranty FAQ.

(2) If you purchased the product directly from Cisco, call Cisco TAC by phone to start a validation of your warranty claim. To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL: <https://www.cisco.com/go/DirTAC>

(3) Cisco's Technical Assistance Center (TAC) will perform limited troubleshooting to isolate the Hardware problem and determine cause of failure.

(c) Advance Replacement Products:

(1) All defective parts must be returned in accordance with the Cisco RMA Policy for Warranty and Hardware Support Contract Returns.

(d) Return To Factory Products:

(1) Return the unit to Cisco or your network supplier as instructed. Cisco will ship a replacement part once your defective product is received.

(2) Your unit will be replaced per the applicable warranty guidelines.

(3) If you cannot locate your network supplier, you may return the unit to Cisco.

9. Important claim information you should record.

9.1 Complete the form below and keep for ready reference.

Approved Source Product was purchased from:

Approved Source telephone number:

Product model and serial number:

Maintenance contract number (if applicable):

10. Definitions

<i>Term</i>	<i>Meaning</i>
Approved Source	Cisco, a Cisco Partner, or a fulfillment agent (e.g., public cloud marketplaces) as may be appointed by Cisco from time to time.
Cisco Partner	A Cisco authorized reseller, distributor, systems integrator or other third party authorized by Cisco to sell Cisco Product.
Customer, End User, You or Your	The entity purchasing Services for its own internal use either directly or through an Approved Source.
Documentation	The technical specifications and use materials officially published by Cisco specifying the functionalities and capabilities of the applicable Product as updated from time to time.
Hardware	Tangible Cisco-branded hardware products as generally available on the Price List. Hardware does not include any tangible product listed on the Price List in the name of a third party.
Product	Cisco Hardware and Software products that are made generally available.
Software	Cisco-branded computer programs, including Upgrades and firmware.
Upgrades	All updates, upgrades, bug fixes, error corrections, enhancements and other modifications to the Software.

Online Resources

Cisco General Terms

The General Terms governing software use is attached hereto and available at the following URL:
<https://www.cisco.com/go/softwareterms>.

Warranty Online

Product warranty terms and other information applicable to Cisco products are available at the following URL: <https://www.cisco.com/go/warranty>.

Cisco 90-Day Limited Software Warranty

WARR-90-DAY-SW-TS

Limited Warranty and Disclaimer

- a. **Limited Warranty.** Cisco warrants that the Software will substantially conform to the applicable Documentation for the longer of (i) ninety (90) days following the date the Software is made available to You for your Use or (ii) as otherwise set forth at <https://www.cisco.com/go/warranty>. This warranty does not apply if the Software, Cisco product or any other equipment upon which the Software is authorized to be used: (i) has been altered, except by Cisco or its authorized representative, (ii) has not been installed, operated, repaired, or maintained in accordance with instructions supplied by Cisco, (iii) has been subjected to abnormal physical or electrical stress, abnormal environmental conditions, misuse, negligence, or accident; (iv) is licensed for beta, evaluation, testing or demonstration purposes or other circumstances for which the Approved Source does not receive a payment of a purchase price or license fee; or (v) has not been provided by an Approved Source. Cisco will use commercially reasonable efforts to deliver to You Software free from any viruses, programs, or programming devices designed to modify, delete, damage or disable the Software or Your data.
- b. **Exclusive Remedy.** At Cisco's option and expense, Cisco shall repair, replace, or cause the refund of the license fees paid for the non-conforming Software. This remedy is conditioned on You reporting the non-conformance in writing to Your Approved Source within the warranty period. The Approved Source may ask You to return the Software, the Cisco product, and/or Documentation as a condition of this remedy. This Section is Your exclusive remedy under the warranty.
- c. **Disclaimer.** Except as expressly set forth above, Cisco and its licensors provide Software "as is" and expressly disclaim all warranties, conditions or other terms, whether express, implied or statutory, including without limitation, warranties, conditions or other terms regarding merchantability, fitness for a particular purpose, design, condition, capacity, performance, title, and non-infringement. Cisco does not warrant that the Software will operate uninterrupted or error-free or that all errors will be corrected. In addition, Cisco does not warrant that the Software or any equipment, system or network on which the Software is used will be free of vulnerability to intrusion or attack.
- d. **Limitations and Exclusions of Liability.** In no event will Cisco or its licensors be liable for the following, regardless of the theory of liability or whether arising out of the use or inability to use the Software or otherwise, even if a party been advised of the possibility of such damages:
 - (a) indirect, incidental, exemplary, special or consequential damages; (b) loss or corruption of data or interrupted or loss of business; or (c) loss of revenue, profits, goodwill or anticipated sales or savings. All liability of Cisco, its affiliates, officers, directors, employees, agents, suppliers and licensors collectively, to You, whether based in warranty, contract, tort (including negligence), or otherwise, shall not exceed the license fees paid by You to any Approved Source for the Software that gave rise to the claim. This limitation of liability for Software is cumulative and not per incident. Nothing in this Agreement limits or excludes any liability that cannot be limited or excluded under applicable law. The foregoing limitation of liability shall not apply to (1) personal injury or death resulting from Licensor's negligence; (2) for fraud; or (3) for any other matter for which liability cannot be excluded by law.

Glossary

“Approved Source” means (i) Cisco or (ii) the Cisco authorized reseller, distributor or systems integrator from whom you acquired the Software.

“Cisco” means Cisco Systems, Inc. or its affiliates

“Documentation” is the Cisco user or technical manuals, training materials, specifications or other documentation applicable to the Software and made available to You by an Approved Source.

“Entitlement” means the license detail; including license metric, duration, and quantity provided in a product ID (PID) published on Cisco’s price list, claim certificate or right to use notification.

“Software” means the Cisco computer programs and any Upgrades made available to You by an Approved Source and licensed to You by Cisco.

“Upgrades” means all updates, upgrades, bug fixes, error corrections, enhancements and other modifications to the Software and backup copies thereof.

“Use” or **“Using”** means to download, install, activate, access or otherwise use the Software.

“You” and **“Your”** means the individual or legal entity licensing the Software under the Cisco General Terms (<https://www.cisco.com/go/softwareterms>).

Governing Law, Jurisdiction and Venue

If You acquired the Software in a country or territory listed below, as determined by reference to the address on the purchase order the Approved Source accepted, this table identifies the law that governs this Limited Warranty (notwithstanding any conflict of laws provision) and the specific courts that have exclusive jurisdiction over any claim arising under this Limited Warranty.

(a) If You are a US State, Local and Education Government end user, these terms, and any disputes arising from them, are subject to the laws of the primary jurisdiction in which You are located.

(b) If You are a US Federal Government end user, these terms, and any disputes arising from them, are subject to the Federal laws of the United States.

The parties specifically disclaim the application of the UN Convention on Contracts for the International Sale of Goods. In addition, no person who is not a party to the General Terms shall be entitled to enforce or take the benefit of any of its terms under the Contracts (Rights of Third Parties) Act 1999. Regardless of the above governing law, either party may seek interim injunctive relief in any court of appropriate jurisdiction with respect to any alleged breach of such party's intellectual property or proprietary rights.

Online Resources

Cisco General Terms

The Cisco General Terms governing software use is available at the following URL:

<https://www.cisco.com/go/softwareterms>.

Warranty Online

Product warranty terms and other information applicable to Cisco products are available at the following URL: <https://www.cisco.com/go/warranty>.

Consult the above website or your Cisco Sales and Service Representative for a complete listing of Cisco products and applicable warranties.



Cisco Systems Inc.

Services Supplemental Terms

In this document:

- Services Guide
- Cisco Services with US Government
- Cisco Severity and Escalation Guidelines
- Support Reinstatement Policy
- Cisco Non-Entitlement Policy (External) Version 2.0
- Terms of Use: Cisco Customer Experience Cloud
- Virtual Visitation Service: Service Summary



Website references

Throughout the Cisco terms, references to external websites will instead point to attachments included in this package. Links and webpage references in the left column shall mean the document (and section) in the right column.

<i>Link / Reference</i>	<i>Document / Section</i>
Warranties Product Warranties https://www.cisco.com/go/warranty	General Terms & Appendices, Warranty section
Cisco General Terms webpage Software General Terms	General Terms & Appendices,
Data Protection Agreement	General Terms & Appendices, Data Protection Agreement section
Information Security Exhibit	General Terms & Appendices, Information Security Exhibit section
Customer Content – Data Brief webpage	General Terms & Appendices, Customer Content: Data Brief section
Personal Data – Data Brief	General Terms & Appendices, Personal Data: Data Brief section
Systems Information – Data Brief	General Terms & Appendices, Systems Information: Data Brief section
Cisco Software Transfer and Re-licensing Policy http://network.cisco.com/en/US/prod/cisco_software_transfer_relicensing_policy.html .	General Terms & Appendices, Software Transfer and Re-licensing Policy section
Software Portability Policy Software License Portability Policy	General Terms & Appendices, Software License Portability Policy section
https://www.cisco.com/go/softwareterms https://network.cisco.com/c/en/us/products/end-user-license-agreement.html	General Terms & Appendices Appendix - Offer Descriptions - Products
Cisco RMA Policy for Warrant and Hardware Support Contract Returns	General Terms & Appendices, RMA section
Offer Descriptions Product Specific Terms Product Descriptions Product Offer Descriptions	Follow to website via URL in document
Offer Descriptions Service Specific Terms Service Descriptions Service Offer Descriptions Software Support Service Solution Support	Follow to website via URL in document

Services Guide

During the Services Term, You will receive Services in accordance with the relevant Service Description or SOW, this Services Guide, applicable Services policies, and Your Services Agreement.

To help us make the Services successful, we need You, Your teams, facilities, and equipment to be ready, available, and responsive; if not, we may be prevented from or delayed in performing the Services or delivering the expected outcomes and You will be responsible for any costs we incur.

1. General

1.1. Customer Responsibilities:

You are responsible for use of and access to the Services, Software, and any Cisco hosted portals or tools by Your identified agents, Approved Sources, and personnel.

You are responsible for Your own information security and data privacy. Please backup and protect Your data against loss, damage, theft, or destruction.

You are responsible for the determination of Your Network design, business, regulatory compliance, security, privacy, and other requirements, including whether to follow guidance or recommendations provided as part of the Services.

You will:

- (a) identify a lead contact to address any issues identified during the Services Term;
- (b) have the appropriate people at any meetings, workshops and interviews who can respond to issues identified and who can access the Services and download Software on Your behalf, if required;
- (c) provide prompt and accurate responses (e.g. within 2 Business Days) to information requests, such as Services entitlement and install base/license data, relevant updates or changes planned to Your Network;
- (d) ensure Your facilities are available and ready for delivery of the Services, including by providing authorizations, necessary and safe access to equipment, and connectivity, and any necessary change/maintenance window(s);
- (e) manage any dependencies with Your other equipment or software, and/or with any third parties;
- (f) take the necessary steps to protect Your Network when deploying recommended software updates or making configuration changes;
- (g) ensure Cisco representatives are not treated as Your own employees;
- (h) use any Hardware, Software or other materials (e.g., Data Collection Tools) that Cisco provides You according to their applicable license terms during the Services Term, allow Cisco reasonable access to replace or update them, and return them to Cisco (or fully delete them, as Cisco directs) at the end of the Services Term or when requested;
- (i) assign a proposed Severity Level for issues reported to us according to the [Severity and Escalation Guidelines](#);
- (j) assist in troubleshooting Hardware prior to initiating an RMA request;
- (k) use the latest release of Cisco or third-party software, if we advise You that it will address a reported Software problem; and
- (l) ensure the security of your chosen delivery methods for the transmission of Deliverables to You, the use of which shall be at Your own risk.

1.2. Cisco Responsibilities:

Cisco will:

- (a) identify a lead contact and relevant personnel, at Cisco's discretion, as needed during the Services Term;
- (b) perform Services remotely during Standard Business Hours unless otherwise stated in a Service Description or SOW;
- (c) provide requirements to You to prepare for and perform the Services;
- (d) provide the Services and Documentation in English and other selected languages at Cisco's discretion using Cisco's designated delivery tools and methods; and
- (e) access, protect, process, and use data in connection with Your use of the Services in accordance with the materials on Cisco's [Trust Center](#).

2. Professional Services

2.1. Contract Change Control Procedures (typically referred to as Change Management Procedures):

- (a) The party requesting a change to the SOW will deliver a written contract change request ("Change Request") to the other party describing the nature of the proposed change(s).
- (b) If both parties agree to the change(s), then both parties must sign the Change Request for the Change Request to be considered an amendment to the SOW.
- (c) If there is a conflict between the original SOW and any executed Change Request, the last fully executed Change Request will prevail with respect to the conflict.

2.2. Completion and Acknowledgement Process:

If a Service or a specific Document Deliverable is listed for approval in a SOW or Service Description, the parties will use the review process described below:

- (a) Standard of Review. The standard of review is that the Service or Document Deliverable materially complies with the requirements of the applicable SOW or Service Description.
- (b) Notification. For Services requiring Your acceptance, we will notify You in writing that the Service is complete and available for review, and we will provide You with a Milestone Completion Certificate ("MCC") for review. When a Document Deliverable is ready for review and approval, Cisco will present and review the Document Deliverable with You.
- (c) Timeframe. The review and approval process must be completed within the following timeframes or as set forth in the applicable SOW or Service Description: (a) Document Deliverables: 2 Business Days from completion of the review by You and Cisco of the Document Deliverable, or (b) Services: 5 Business Days from the date we provide the MCC.
- (d) Approvals. You must approve or reject the Service or Document Deliverable in writing within the timeframe listed above or the Service or Document Deliverable will be considered accepted and completed. If we provide You with a MCC, signing the MCC (or taking no action in the timeframe listed) will signify acceptance of the Services. If You reject a Service or Document Deliverable, Your written rejection must also include detailed reasons as to why the Service or Document Deliverable does not meet the standard above. If continuing performance of the Services is dependent on an approval, then the impacted Services may be delayed or suspended until approved or otherwise resolved. Your acceptance or rejection as described in this Section is not an acceptance or rejection of any Products, subscription, or other Services purchased or licensed by You.
- (e) Resubmission. If the rejected Service or Document Deliverable does not meet the standard of review referenced above, we will address the stated reasons for the rejection in a timely manner by reperforming the rejected portion(s) of the Service or resubmitting the Document Deliverable so that the Service or Document Deliverable meets the standard of review referenced above. After we notify You that the rejected Service is complete or we resubmit the Document Deliverable to You, then this review process will begin again and be repeated as before with respect to the basis for Your rejection. The Document Deliverable review and approval process is limited to 2 review and approval cycles.

- (f) Responsible Party. If the Services was sold directly by us to You, then the acknowledgment process detailed above will be used by us and You, with You responsible for reviewing the Service. If the Services was sold through a Cisco Partner, then the acknowledgment process detailed above will be used by us and the Cisco Partner, with the Cisco Partner responsible for the review and approval process described in this section.

3. Incidental materials and technology

Generally, Cisco does not include Software or Scripts in our Services and You must purchase them separately. However, if Cisco provides Software and/or Scripts as part of the Services, these are:

- (a) provided incidental to the provision of Services; and
- (b) licensed to You solely for the purposes of the Services and according to the [General Terms](#) or any applicable Service Description.

Cisco will provide Software and/or Scripts in object code unless the SOW or Service Description states otherwise. If Cisco provides You with access to Source Code for any incidental Software and Scripts, then the Source Code (including any copies, modifications, enhancements, and derivative works of the Source Code) is Cisco Confidential Information and is licensed to you in accordance with Cisco's [Sample Code License](#).

Incidental Software and Scripts, as well as any other third-party materials (e.g., cables, racks, test equipment, etc.) that we provide to You incidental to provision of the Services, are provided "AS-IS" and without warranty, support, or maintenance.

4. Contracting with U.S. Federal Government

For Services engagements related to a U.S. Federal Government contract, the following terms are applicable to the purchase of the Services from Cisco: [Cisco Services with US Government](#).

5. Glossary

The following are defined terms we most often use in our Service Descriptions, SOWs and related documents. Additional terms may be defined in the General Terms, Cisco policies, or specific Service Descriptions.

Defined Term	Meaning
Advance Replacement	Shipment of new or equivalent to new, at Cisco's sole discretion, replacement Field-Replaceable Unit (FRU) before receiving failed FRU.
Application Software	Non-resident or standalone Software Products listed on the Price List or in the Cisco cloud.
Business Days	The generally accepted days of operation per week within the country where the Services are performed, excluding local holidays.
Business Hours	9:00 AM to 5:00 PM, Customer's local time, on Business Days for the performance of Services. For replacement of failed Products, Business Hours are 9:00 AM to 5:00 PM Local Depot Time on Business Days.
Customer	The entity purchasing Services for its own internal use from the Approved Source. Includes Customer, End User, You or Your.
Data Collection Tools	All hardware and/or software tools that support Cisco's ability to collect Network information, provide troubleshooting on cases, data analysis, and report generation capabilities as part of the Services.
Deliverable(s)	Items to be delivered by Cisco as set forth in an applicable Service Description, including without limitation any Software, Reports, Data Collection Tools, and/or Scripts.
Document Deliverable(s)	Items identified as such within a SOW or relevant Service Description and which will also be subject to the Completion and Acknowledgement Process outlined in Section 2.3 of these terms.
Event	Notification by Customer of its performance of a planned Network, Hardware, Software, or configuration change.
Feature Set Upgrade	A separately licensed and priced Software release that contains an enhanced configuration or feature set.
Field-replaceable Unit (FRU) or Service Part	Any component or subassembly of an item or unit of Hardware that is new or equivalent to new, in Cisco's sole discretion, and that reasonably can be replaced at Customer's location. FRUs also may be subject to size and weight limitations.
Local Depot Time	Central European Time for Services provided in Europe-Middle-East and Africa, Australia's Eastern Standard Time for Services provided in Australia; Japan's Standard Time for Services provided in Japan and Pacific Standard Time Services provided in all other locations.
Network or Environment	A set of interconnected Cisco supported Hardware and Software (or its components) to which the Services apply.
Product	Cisco Hardware and Software products that are made generally available.
Purchase Order or PO	A written or electronic order to Cisco for the Services to be provided by Cisco under the Services Agreement.
Quote	The valid Cisco quote to be referenced on the PO for the associated Services to be purchased, which would be issued between Cisco and Customer for direct purchases, or between Cisco and your Cisco Partner (with corresponding quote and PO between the Cisco Partner and Customer).
Reports	Reports, recommendations, network configuration diagrams, and related non-Software Deliverables made available by Cisco as part of a Service.
Response Time	For Advance Replacement Services, the period commencing on the creation of the RMA request and ending when the FRU is delivered On Site; for On Site Services, the period commencing on creation of the RMA request and ending when Cisco personnel arrive On Site.

Same Day Shipment	Local Same Day Shipment (SDS) or International SDS is available where Next Business Day (NBD) or Next Calendar Day Service (NCD) cannot be provided. RMA will be dispatched from the closest In Country/International regional depot. For international RMA shipments, Customer will be responsible to act as the Importer of Record (IOR), liable for any destination charges such as duties/taxes and any other local regulatory licenses or permits for the country of import.
Scripts	Software scripts, macros and batch files provided by Cisco.
Service(s)	One or more of the Cisco services options purchased by an Approved Source or Customer, as applicable.
Services Agreement	○ If You purchased the Services directly from Cisco: Your Master Services Agreement, Advanced Services Agreement, or other equivalent agreement applicable to the purchase of the Services with Cisco. If no Master Agreement exists as described above, then the applicable Services Agreement will be as follows: • For Service Descriptions: The General Terms. • For SOWs: The SOW Terms and Conditions. ○ If You purchased the Services from an authorized Cisco Partner for Internal Use: The agreement between You and Your Cisco Partner applicable to the purchase of the Services from Cisco. ○ If You are a Cisco Partner and You purchased the Services for resale to customers/end user: The Distributor Agreement, Systems Integrator Agreement, Indirect Channel Partner Agreement or equivalent agreement applicable to the resale of the Services.
Service Description	A description of the business and technical terms of the applicable Service. A Service Description provides an overview of the relevant Service and any additional terms related to the Service.
Service(s) Term	The duration of the Service purchased as set forth in the Quote. All included Services and Deliverables are available for consumption solely during the same Services Term in which such Services and Deliverables are purchased. References in Service Descriptions to Services being provided during a “year” (e.g., quantities such as “once a year”) or otherwise on an annual basis mean a Service Term year and not a calendar year, unless expressly stated otherwise.
Severity Levels	See the Severity and Escalation Guidelines .
Software Releases	• Maintenance Release is an incremental Software release that provides maintenance fixes and may provide additional Software functions. Cisco designates Maintenance Releases as a change in the digits to the right of the tenths digit or of the hundredths digit of the Software version number [x.x.(x) or x.x.x.(x)]. • Minor Release is an incremental release of Software that provides maintenance fixes and additional Software functions. Cisco designates Minor releases as a change in the tenths digit of the Software version number [x.(x).x]. • Major Release is a release of Software that provides additional software functions. Cisco designates Major Releases as a change in the ones digit of the Software version number [(x).x.x].
Source Code	Software code in human-readable or non-compiled form, including any programmer’s notes, related materials and Documentation.
Statement of Work or SOW	The documents agreed upon by the parties that define professional Services (exclusive of maintenance and support), if any, to be provided by Cisco.
TAC	The Cisco Technical Assistance Center.

6. Applicable Links

[Service Descriptions for Cisco Services and related policies](#) [General Terms](#)

Cisco Services with US Government

For Federal Government agencies, Cisco Services offerings are considered “commercial items” as defined under the Federal Acquisition Regulation (“FAR”) 2.101. Cisco offers and/or provides these Services upon a competitive basis and in substantial quantities in the commercial marketplace based upon established market prices for specific tasks performed under standard commercial terms and conditions.

When Cisco Services require access to US Government classified information, resources, the following shall apply:

Cisco will:

- a. Meet security requirements for access to classified information as specified in the Department of Defense (DD) Form 254, Department of Defense Contract Security Classification Specification, and attachments.
- b. Obtain and retain a Facility Clearance in accordance with the DD Form 254 and FAR 52.204-2 “SECURITY REQUIREMENTS.”
- c. Perform the following activities pursuant to applicable US Government and agency guidelines:
 - i. Appoint a Facility Security Officer (FSO) to oversee the security requirements for contract deliverables and services.
 - ii. Appoint a FSO to oversee clearance processing and debriefings of Cisco employees and subcontractors.
 - iii. Educate and train Cisco employees and subcontractors.
 - iv. Provide safe storage of documents, material, or information provided under the contract.
 - v. Protect documents, material, or information provided under the contract, in transit and at rest.
 - vi. Assist in preparation of security documentation.

Customer will:

- a. Perform the following activities pursuant to applicable US Government and agency guidelines:
 - i. Provide a DD Form 254 Contract Security Classification specification with DD Form 254 flow downs and attachments.
 - ii. Ensure the proper security classification markings for all documents, materials, or information.
 - iii. Manage assignment of personnel to the contract.

Cisco Severity and Escalation Guidelines

When You are submitting a problem to Cisco, assign a Severity Level as follows:

Table 1. Severity Levels

<i>Severity Level</i>	<i>Description</i>
Severity 1	Critical impact on the customer's business operations. Cisco's hardware, software or as a service product is down.
Severity 2	Substantial impact on the customer's business operations. Cisco hardware, software or as a service product is degraded.
Severity 3	Minimal impact on the customer's business operations. Cisco hardware, software or as a service product is partially degraded.
Severity 4	No impact on the customer's business operations. The customer requests information about features, implementation, or configuration for Cisco's hardware, software, or as a service product.

Cisco and You will commit resources and provide requested information in accordance with the corresponding Severity Levels:

- Severity Level 1: Full-time resources
- Severity Level 2: Full time resources during Business Hours
- Severity Level 3: Resources during Business Hours
- Severity Level 4: Resources during Business Hours to provide information

If You do not believe that adequate problem resolution progress is occurring, You may use the following procedure to escalate and connect directly with a resolution owner.

Please escalate using: (1) the Cisco Support Assistant at <https://supportassistant.cisco.com/escalate>, (2) the Webex App, (3) the [Support Case Manager](#), or (4) Virtual Spaces.

You will need to:

- Enter case number
- Provide escalation reason
- Choose "Escalate to TAC Manager"
- Provide phone number for Severity 1/Severity 2 case or email address for Severity 3/Severity 4 case

Support Reinstatement Policy

Updated: January 2023

Purpose

This document sets forth Cisco's policy regarding reinstating Support on Products that have lapsed or have never been covered. Support provides Customers (a) entitlement to download, deploy and use applicable Software updates, (b) hardware replacement, and (c) access to Cisco's Technical Assistance Center (TAC). Customers whose Support has lapsed or who have not previously purchased Support will need to establish or re-establish Support in order to obtain TAC support, Software updates, and / or Hardware replacements (for Products or Support levels not entitled under warranty). Customers seeking to reinstate Support may be subject to reinstatement fees and such Products may require inspection and Software relicensing prior to Support reinstatement.

This policy applies to sales of Support on Products—whether renewed or new, Customer entitled or partner entitled—through Cisco's Authorized Channel Network. This policy applies to all regions of operation.

Counterfeit and pirated products cannot be covered by Support. Unauthorized Products cannot be covered or reinstated until they have been inspected and relicensed.

Definitions

For purposes of this policy, the following definitions apply:

1. **"Authorized Channel Network"** means Cisco sales directly to end user Customers; Cisco sales to Cisco Channel Partners (who sell directly to end user Customers, or within the European Economic Area (EEA) also to other Cisco Channel Partners or Distributors); and Cisco Distributors (who sell to Cisco Channel Partners who resell to end user Customers, or within the EEA also to other Cisco Channel Partners or Distributors) where the purchasers of such product are within the contractually agreed territories for the Cisco Channel Partner or Distributor in question.
2. **"Customer"** means the entitled party of the Support, whether an end Customer who has purchased from Cisco or the Authorized Channel Network, or an Authorized Channel partner who has purchased Support which they will incorporate into their own offers.
3. **"Decommissioned"** means any instance of a Product that is no longer in use in Customer's network following notice to Cisco by Customer.
4. **"Hardware"** means Cisco-branded hardware, including tangible Cisco equipment, devices, or components made available.
5. **"Inactive"** means the Product will no longer be entitled to Support, will not be eligible to be added to Support through standard quoting and order processes nor will be identified in Cisco's inventory discovery.
6. **"Product"** means Hardware and Software that are made generally available.
7. **"Software"**
 - a. means the object code version of the computer programs listed on Cisco's published global price list or provided with Hardware, whether operating system Software or application Software, including copies, bug fixes, updates and upgrades thereof. Operating System (OS) Software generally refers to Software that is required to operate a device (examples include IOS and IOS- XR). Application Software generally refers to Software that runs an application (examples include call center, unified messaging and network management Software). Software does not include any computer programs listed on Cisco's published global price list in the name of a third party.

- b. Software provided by Cisco, including any copies, updates, upgrades, modifications, enhancements, and any derivative works thereof.
- 8. **“Support”** means the entitlement to access technical support, and to download, deploy and use applicable software updates for the covered Product—whether Hardware or Software, purchased from an Authorized Channel Network.
- 9. **“Unauthorized Product” means** New or used Products that are sourced and/or sold outside Cisco’s Authorized Channels Network.

Support Reinstatement Policy

This policy governs the reinstatement of Support. Hardware inspection and/or Software relicensing may be required prior to reinstatement. Please refer to the [Software License Transfer and Re-Use Policy](#) for further details.

1. Support Reinstatement

1.1 Support Reinstatement Requirements:

1.1.1 Support purchased more than ninety (90) days after original Product ship date is subject to reinstatement.

1.1.2 Support which has expired and is more than thirty (30) days overdue for renewal is subject to reinstatement.

1.2 Additional Support Reinstatement Requirements:

1.2.1 Cisco customers must purchase at least one (1) year of Support on any Software licensed for a perpetual term, within ninety (90) days of the associated date of sale.

Support purchased after the 90-day grace period may be subject to reinstatement fees from the date of Software purchase.

1.2.2 Decommissioned Products will be put into an Inactive status in Cisco’s database.

1.2.3 Decommissioned Products may be subject to reinstatement fees before being added to Support.

1.3 Software Relicensing: Where the current owner of the Product is not the licensed end user, relicensing fees may be required prior to the initiation of the reinstatement process.

1.4 Inspection: Where there is a lapse in Support of ninety (90) days or more, an inspection and associated fees may be required prior to initiation of the reinstatement process.

1.5 Reinstatement Fee: A reinstatement fee may be required in order to add or renew Support. The reinstatement fee is non-refundable fee and does not apply to the purchase of any Support. The reinstatement fee is calculated as: (Number of Days Lapsed x Support Daily Rate) + 10% or 20% fee.

1.6 Last Day of Support (LDoS).

1.6.1 No reinstatement of Support will be allowed after Last Day of Support. Please check services availability on the [Cisco End-of-Sales and End-of-Life Product](#) website for details.

1.6.2 Renewal beyond the End of Sale announcement for a product with a defined migration path is not encouraged and the reinstatement of such products will not be allowed. When End of Sale for a product or service has been announced and a migration path defined, if the end of term of a subscription or service contract for that product is reached without it being renewed on time it will not be eligible for reinstatement.

1.7 Support Eligibility:

Products where the above inspection, Software License and reinstatement requirements have been met will be eligible to purchase Support on the then current Global Price List, subject to regional availability.

Cisco Non-Entitlement Policy (External) Version 2.0

1. General Conditions

You are solely responsible for maintaining an inventory of Products and Software ("Installed Base") necessary to establish entitlement to Services. Cisco may assist You with maintaining an up-to-date Installed Base inventory by making available My Cisco Entitlements self-help tools.

1.1 Services or Warranty entitlements that are not expressly set forth in the applicable Service Description or Warranty document are not covered under such Services Description or Warranty entitlement including, without limitation, the following:

(a) Support or replacement of a Product that is altered, modified, mishandled, destroyed, or damaged by one or more of the following:

- (1) natural causes;
- (2) environmental failures;
- (3) Your failure to take any required actions;
- (4) a negligent or willful act or omission by You or use by You other than as specified in the applicable Cisco-supplied Documentation;
- (5) intentional permanent cosmetic alterations;
- (6) an act or omission of a third party.

(b) Support or replacement of Product that was inoperable prior to purchase of a maintenance contract with Cisco.

(c) Support of Product beyond the identified Last Day of Support ("LDoS") date, regardless of whether such Product has been included in any chassis-based service pricing.

(d) Services for Products:

- (1) for which a valid maintenance contract is not in place; or,
- (2) Services or Warranty coverage for Products with an expired Warranty coverage date and no active Service contract.

(e) Services for a Product that Cisco determines is Non-Genuine Product. Any warranty support or Services for a Product determined to be a Non-Genuine Product is void. Cisco reserves the right to immediately terminate any associated support service contract or Warranty, and any replacement parts or other materials made available in connection with that Non-Genuine Product must be returned to Cisco.

(f) Services and Warranty are only provided for generally available Products and Software releases/versions.

(g) Services or software to resolve Software or Hardware problems resulting from third-party product(s) or causes beyond Cisco's control.

(h) Furnishing of supplies, accessories, or the replacement of expendable parts (e.g., batteries, cables, blower assemblies, power cords, and/or rack mounting).

(i) Cisco uses solid-state drives from various vendors. All solid-state drives are subject to physical write limits and have varying maximum usage limitation specifications set by the manufacturer. Cisco will not replace any solid-state drives that have exceeded any maximum usage specifications set by Cisco or the manufacturer, as determined solely by Cisco.

(j) Hardware replacement in quantities greater than three (3) FRUs, including those replacements due to pervasive issues documented in an engineering change notice or field alert unless End User has troubleshoot each failed Hardware down to the FRU level.

- (k) Any Hardware or Third-Party Product upgrade required to run new or updated Software.
- (l) Any customization of, or labor to install, Software and Hardware (including installation of updates).
- (m) Erasure or removal of any of Your or third-party data on Products (or parts thereof) returned, repaired, or otherwise handled by Cisco.
- (n) Services for Product where service contract was purchased from a source other than Cisco or its Authorized Channel.
- (o) Services for Product where Cisco Software license(s) deposited on Smart Licensing platform associated with the Product were purchased, modified, or otherwise used in violation of the applicable terms. Cisco reserves its right to:
 - (1) invoice the party for the authorized Cisco Software license; and,
 - (2) pursue other available remedies, including termination of Services, as well as Cisco user profiles and access rights.

2. Deployment and Delivery

Cisco provides support for our installed products in commercial or governmental locations not requiring specialized access equipment and meeting all local safety regulations. Products are delivered to the normal postal delivery address or freight dock by regulated delivery services. Cisco does not provide:

- 2.1 Services for Products that are (a) installed outdoors or (b) installed indoors but require specialized equipment to perform such Service. Cisco will not supply specialized access equipment and will not perform Service until You provide access that meets applicable local labor laws and workplace safety rules for Cisco employees and contractors.
- 2.2 Services performed at domestic residences.
- 2.3 Any expenses incurred to visit End User's location, except at Cisco discretion during escalation of problem resolution by Cisco.
- 2.4 Electrical or site work external to the Products. This also excludes any installation staff, such as a licensed electrician for direct interconnect of power, or installation work not covered by a specific installation contract SOW.

3. Software

Cisco provides support for selected software products and Third-Party solution components. Cisco does not provide:

- 3.1 Services on non-authorized software.
- 3.2 Warranty or Service coverage for Product or Software support, including updates and bug fixes for which (a) a valid license for the Product is not in place or (b) Product which was purchased from a source other than Cisco or its Authorized Channel. Cisco reserves the right to: (1) suspend support associated with such Products until such time as any applicable inspection is conducted and any applicable relicensing fees are paid for such Products or (2) terminate the support service contract and/or Warranty.
- 3.3 Support for any Software release that has reached LDoS.
- 3.4 Open Source, community-supported project software.

4. Cloud and Remote Software Services

<Reserved>

5. Non-Cisco Hardware and Software

Cisco may, as part of authorized Solutions, support use of authorized Third-Party components and SW products. Those items shall be specified in the individual Solution Service Description. Cisco does not support:

5.1 Third-Party Components. The Cisco guideline for support and warranty services for the use of non-authorized third-party memory, cables, interface modules, filters, or other non-Cisco authorized components is as follows:

(a) When You report a product fault or defect and Cisco believes the fault or defect can be traced to the use of third-party memory products, cables, interface components, filters, or other non-Cisco authorized components by You or a reseller, then, at Cisco's discretion, Cisco may withhold support under warranty or a Cisco support program. If Cisco concludes that the fault or defect is not attributable to the use of third-party memory, cables, interfaces, filters, or other non-Cisco authorized components installed by You or a reseller, Cisco will continue to provide support for the affected product under warranty or covered by a Cisco support program.

(b) Cisco also reserves the right to charge You for services provided to You when Cisco determines, after having provided such services, that the root cause of the defective product was caused by a non-supported third-party vendor supplied product.

5.2 Third party repairs or repair components are also grounds for Cisco to cancel service or warranty support. Cisco may pursue recovery of parts provided to replace product later found to have previous third-party repairs or components.

6. Non-Genuine, Destroyed, or Stolen Product

This section sets forth the invalidity of warranty and service support for any Destroyed, Stolen, or Scrapped Product. This policy is intended to support and be consistent with other relevant Cisco policies, such as those regarding Cisco trademarks and copyright materials, Software Licensing, Non-Genuine Products, programs that permit Cisco's Authorized Channel to sell legitimate and genuine Products and Services, and any other Cisco policies referenced in this policy.

6.1 Warranties. Cisco does not offer any kind of warranty support for Destroyed, Stolen, or Scrapped Products. None of Cisco's written warranties (as set forth at <https://network.cisco.com/c/en/us/products/warranty-listing.html> or elsewhere) applies to any Destroyed, Stolen, or Scrapped Products.

6.2 Services. Cisco does not offer for sale or otherwise any Services for Destroyed, Stolen, or Scrapped Products. None of Cisco's service offerings applies to any Destroyed, Stolen, or Scrapped Products.

6.3 All service contracts and/or Hardware or Software warranty obligations pertaining to Destroyed, Stolen, or Scrapped Products are void. Upon Cisco's discovery and verification of products as Destroyed, Stolen, or Scrapped Products, Cisco will immediately terminate all associated Services and/or warranty support for such Destroyed, Stolen, or Scrapped Products, and may take other available actions. You are not entitled to a refund for associated termination of support for Destroyed, Stolen, or Scrapped Products.

6.4 Refurbished Equipment. Cisco does not offer Services, or authorize or endorse any third party, to refurbish any Destroyed, Stolen, or Scrapped Products. Cisco's Authorized Refurbished Equipment Program (located at <https://network.cisco.com/c/en/us/buy/cisco-capital-finance/refresh/overview.html>) and related Software licensing (located at <https://network.cisco.com/c/en/us/products/network-sw-relicensing-program.html#~policy#~using>) do not apply to any Destroyed, Stolen, or Scrapped Products. Inspections. Cisco does not offer, authorize, or endorse any used equipment inspection or recertification for Destroyed, Stolen, or Scrapped Products.

6.5 Return Material Authorization. Cisco does not accept Destroyed, Stolen, or Scrapped Products as a part of Cisco's RMA process for Advance Replacements. Destroyed, Stolen, or Scrapped Products sent to Cisco either directly or via a Cisco-Authorized Channel will not qualify as meeting Cisco's RMA requirements.

6.6 Any Cisco product that has been identified as a Destroyed, Stolen, or Scrapped Product (per serial number) will be appropriately identified in Cisco's databases as ineligible for any kind of warranty or service support.

6.7 Any otherwise valid warranty support or Services for a Cisco product that becomes subject to destruction, reported theft, or scrapping will immediately become void and terminate upon such destruction.

6.8 Cisco does not have any obligation or liability for Destroyed, Stolen, or Scrapped Products.

6.9 If, per Cisco's Advance Replacement Services or Warranty support, You receive a replacement product from Cisco and then improperly return to Cisco a Destroyed, Stolen, or Scrapped Product (instead of the actual matching serial number defective Product for which the Advance Replacement product was provided), Cisco retains the right to invoice You for a genuine Cisco replacement product, and may take other actions, including, termination of the Your support contract and/or pursue other available actions or otherwise fail to return the specified RMA Product.

6.10 Cisco encourages the removal of all Destroyed, Stolen, or Scrapped Products from Your Network in order to eliminate or reduce risks associated with keeping such Destroyed, Stolen, or Scrapped Products in the Network.

6.11 Destroyed, Stolen, or Scrapped Products are ineligible for Cisco Software licensing agreements or any other assignments of Cisco Operating License rights.

7. Non-Entitlement to Cisco Warranty and Service Support of Unauthorized Products and Illegally Imported Products

7.1 Services and Warranty. Illegally Imported Products and Unauthorized Products are not eligible for Cisco warranties. Illegally Imported Products are ineligible for support services. Unauthorized products may only become eligible for support services following a successful physical inspection and appropriate proof to Cisco showing that any applicable appropriate Software license fees have been paid for the said Unauthorized Products (or that payment is made for such licenses if no prior payment has been made) by or on behalf of the End User who will be using the Unauthorized Products in question. Fees, such as those for reinstatement of services, may apply.

7.2 Refurbished Equipment. Cisco does not authorize or endorse any third party to refurbish Unauthorized Products. However, Cisco does offer refurbished products for sale through the Cisco Authorized Refurbished Equipment Program. Information about the program is available at: <https://network.cisco.com/c/en/us/buy/cisco-capital-finance/refresh/overview.html> Information about Cisco's Software License Transfer and Re-Use Policy is available at: http://network.cisco.com/en/US/prod/cisco_software_transfer_relicensing_policy.html.

7.3 Inspection Fees. Contact your local Cisco service account representative for more information about Cisco's inspection fees and process.

7.4 Software Support. You may only download, install, and expect support for Software versions and feature sets for which they have purchased a valid license that is current and active. By installing, downloading, accessing, or otherwise using such software updates, You agree to follow the terms of the currently published Cisco General Terms. In most cases, the Software Update will be a maintenance release to software that was previously purchased. Free security software updates do not entitle You to a new software license, additional software feature sets, or major revision upgrades.

7.5 Any Illegally Imported Product is ineligible for any Cisco warranty, service, or software support. Any Unauthorized Product is ineligible for any kind of Cisco warranty. Any Unauthorized Product is ineligible for any service, or software support unless it becomes eligible through inspection, applicable licensing, and/or other applicable processes. Cisco reserves the right to terminate any service contract or deny service coverage on Illegally Imported Products and Unauthorized Product. Cisco reserves the right not to issue any refund associated with termination of service contracts on Illegally Imported and Unauthorized Products.

7.6 Cisco assumes no obligation or liability for Unauthorized Products, except as detailed in service contracts written after such Products have been inspected and appropriate Software licenses have been purchased.

Cisco may:

- (a) invoice You for the genuine Cisco replacement Product; and/or,
- (b) pursue other available actions, such as termination of the Your support contract when You:
 - (1) receive a replacement product from Cisco; and,
 - (2) return an ineligible Unauthorized Product instead of the actual defective Cisco product for which the Advance Replacement Product was provided or anything except the specified Product in the RMA.

7.7 Cisco encourages You to check the source and quality of the Products they purchase, in order to reduce risks of purchasing and using Illegally Imported Products and Unauthorized Products in Your Network. Cisco encourages You to check eligibility of Unauthorized Products for Cisco support and the validity of the applicable Software licenses for those Products.

8. Non-Entitlement to Cisco Warranty and Service Support of Non-Genuine Cisco Products

The integrity of a Your Network is of paramount importance. Cisco's ability to properly support Your Network is premised on the basis that the Cisco products and software in such Network comprise genuine products/software that have not been destroyed, stolen, or otherwise constitute scrapped materials. This policy sets forth the invalidity of any warranty and service support for a Non-Genuine Product. This policy is intended to support and be consistent with other relevant Cisco policies, such as those regarding Cisco trademarks and copyright materials, software licensing, destroyed, stolen and scrapped products, channel partner direct and indirect programs that authorize Cisco Channel Partners to sell legitimate and genuine Cisco products and services, and any other Cisco policies referenced in this policy.

8.1 Warranties. Cisco does not provide any kind of warranty support for Non-Genuine Products. None of Cisco's written warranties (as set forth at <https://network.cisco.com/c/en/us/products/warranty-listing.htm> or elsewhere) applies to any Non-Genuine Products.

8.2 Services. Cisco does not offer for sale or otherwise any kind of services for Non-Genuine Products. None of Cisco's service offerings (as set forth on any of Cisco's Price Lists) applies to any Non-Genuine Products.

8.3 All service contracts and/or Hardware or Software warranty obligations pertaining to Non-Genuine Products are void. Upon Cisco's discovery of any Non-Genuine Products, Cisco will immediately terminate all associated services and/or warranty support for such Non-Genuine Product and may pursue other available legal remedies. No refund will apply for terminating all associated services support for Non-Genuine Products.

8.4 Refurbished Equipment. Cisco does not offer services, or authorize or endorse any third party, to refurbish any Non-Genuine Products. Cisco's Authorized Refurbished Equipment Program (found at <https://network.cisco.com/c/en/us/buy/cisco-capital-finance/refresh/overview.html>) and related software licensing (found at <https://network.cisco.com/c/en/us/products/network-sw-relicensing-program.html#~policy#~using>) do not apply to any Non-Genuine Products. Hence, sections (8.1) and (8.2) above are equally applicable to Non-Genuine Products that have been subjected to any type of refurbishment efforts.

8.5 Inspections. Cisco does not offer, authorize, or endorse any kind of used equipment inspection or recertification for Non-Genuine Products.

8.6 Return Material Authorization. Cisco does not accept Non-Genuine Products as a part of Cisco's Return Material Authorization ("RMA") process for Advance replacements. Non-Genuine Products sent to Cisco either directly or via a Cisco-authorized reseller will not qualify as meeting Cisco's RMA requirements and may be subject to destruction.

8.7 Any Hardware or Software that has been identified as a Non-Genuine Product will be appropriately identified in Cisco's databases as ineligible for any kind of warranty or service support.

8.8 Cisco assumes no obligation or liability for Non-Genuine Products.

8.9 If, per Cisco's Advance Replacement services and warranty support, You receive a replacement Product from Cisco and then improperly returns to Cisco a Non-Genuine Product, Cisco retains the right to invoice You for a genuine Cisco replacement Product. Additionally, Cisco may pursue other available actions, including but not limited to termination of Your support contract.

8.10 Cisco encourages the removal of all Non-Genuine Products from Your Network to reduce risks associated with keeping Non-Genuine Products in the Network.

9. Third-Party Repair Sources: Cisco Warranty and Service Support Implications

Cisco Systems® holds ISO 9000 and ISO 14000 certifications and strives to ensure the highest levels of product quality and Your satisfaction. Cisco® contracts with qualified service repair companies worldwide to maintain ISO certifications and provide End User satisfaction. These companies (as subcontractors to Cisco) provide support in connection with Cisco warranty and service contract obligations.

9.1 Cisco employs the authorized repair companies to evaluate, repair, or replace parts or products, including FRUs. An FRU is any component or subassembly of an item, or unit of a product manufactured by Cisco that can be replaced in the field. Example items include chassis, pluggable modules, power supplies, and product-specific printed circuit board assemblies such as line cards.

9.2 Cisco authorized service repair partners receive specialized, ongoing training to competently provide product evaluation, refurbishment, and testing support. Cisco grants these partners access to certified replacement parts, such as the following:

- (a) Engineering Change Order (ECO) processes for latest updates;

- (b) Test plans and procedures developed by Cisco engineers;
- (c) Dynamic burn-in chambers and profiles;
- (d) Fully integrated, automated, and operational test stations in support of the test; plan, including all commercial test systems required
- (e) Auto test Scripts, which control the testing process and data gathering;
- (f) Test methodologies such as those specific to a product family and defined by Cisco, which would include tests for structural integrity, functionality, optical parametrics, and live traffic; and,
- (g) A quality assurance program that verifies product functions and reliability without compromising Your needs.

10. Third-Party Repair Sources

10.1 Cisco authorized service repair partners should be distinguished from third-party repair businesses who offer their own brand of repair or other services for Cisco Products. The third-party repair businesses referenced here should also be distinguished from Cisco Authorized Channel partners and resellers per Cisco Channel Partner Program.

- (a) Cisco does not offer or provide any warranty for products that are repaired by such third-party service repair businesses. Unauthorized repair voids the Cisco Warranty Entitlement. End Users who elect to use such third-party repair sources do so at their own risk.
- (b) Cisco does not “certify,” “authorize,” “endorse,” or “recommend” any third-party service repair businesses and cannot validate or otherwise comment upon their competencies, capabilities, or qualifications.
- (c) Cisco does not offer or provide any replacement or spare parts to third-party service repair businesses.
- (d) All Cisco software license grants are to End Users and are non-transferable. See Cisco Software General Terms at <https://network.cisco.com/c/en/us/products/end-user-license-agreement.html>, including the provisions that prohibit the transfer, assignment, or sublicense of the license to any other person, or to use the Software on unauthorized or second-hand Cisco equipment.

10.2 When You report a product fault or defect and Cisco determines that the fault or defect can be traced to the use of a third-party repair business, Cisco retains the right to withhold support under warranty or a Cisco support program, such as Smart Net Total Care® services.

- (a) Cisco reserves the right to charge You for services provided to You when Cisco determines, after having provided such services, that the root cause of the defective product was due to a third-party vendor or a third-party-vendor-supplied product. If Cisco concludes that the fault or defect is not attributable to the use of a third-party repair company, Cisco will continue to provide support for the affected product under warranty or covered by a Cisco support program.
- (b) End Users who choose to install or use third-party components including, but not limited to, memory, cables, or pluggable modules, do so at their own risk.
- (c) For more information about Cisco’s Limited Warranty, see: <https://network.cisco.com/c/en/us/products/warranty-listing.html>.

Glossary

1. “Authorized Channel” includes:
 - 1.1 Cisco sales directly to You;
 - 1.2 Cisco sales to Cisco Channel Partners (who sell directly to You, or within the European Economic Area (EEA) also to other Cisco Channel Partners or Distributors); and,
 - 1.3 Cisco Distributors (who sell to Cisco Channel Partners who resell to You, or within the EEA also to other Cisco Channel Partners or Distributors) where the purchasers of such product are within the contractually agreed territories for the Cisco Channel Partner or Distributor in question.
 - 1.4 Note: For Cisco Channel Partners in the EEA, this includes sales to parties within all the EEA.
2. “Cisco Distributors” means Cisco Distributors, Distribution Partners, or Authorized Distributors authorized by Cisco to resell Cisco Equipment in the territory in which the End User is located, as published on the Cisco Distributor Locator, at the following URL:
<https://www.ciscochannelconnect.com/DistiLocator> as updated from time to time by Cisco.
3. “Cisco Channel Partners” means the Cisco Registered, Certified (Gold, Silver, Premier, Select, etc.), and Specialized Partners authorized by Cisco to resell Cisco Equipment in the territory in which the End User is located, as published on the Cisco Partner Locator, at the following URL:
<https://locatr.cloudapps.cisco.com/WWChannels/LOCATR/openBasicSearch.do> , as updated from time to time by Cisco.
4. “Destroyed” means Cisco products that have been determined to have been “destroyed” under any circumstances, and declared as such, including, but not limited to, accident or natural causes (e.g., earthquake, hurricane, fire, flood, or other exposure to adverse environmental conditions) or due to any negligent or wilful or unlawful act or omission to act (including acts of terrorism and/or or exposure to harmful substances, conditions, or materials).
 - 4.1 “Destroyed” can also mean those products that have been identified as “destroyed” by You, authorized Cisco reseller, distributor, or other third party (e.g., insurance carrier for You) that legally takes possession or title to the “destroyed” products, on a Certificate of Destruction that is provided to Cisco.
5. “FRU” means Field Replaceable Unit.
6. “Illegally Imported Product(s)” means new or used Cisco products that are imported into specific country or region without Cisco’s consent, in violation of applicable laws and Cisco intellectual property rights.
7. “Non-Genuine” means any Cisco product:
 - 7.1 to which a Cisco Partner logo, Cisco trademark, service mark or any other Cisco mark has been affixed without Cisco’s express written consent;
 - 7.2 (ii) that have not been manufactured by Cisco or by a licensed manufacturer of Cisco;
 - 7.3 (iii) are produced with the intent to counterfeit or imitate a genuine Cisco Product, or
 - 7.4 (iv) where any form of copyright notice, trademark, logo, confidentiality notice, serial number or other product ident.
8. “Scrapped” means any Cisco product that has reached the end of its useful life or which, for quality control or other reasons, Cisco designates for disposal by Cisco or a Cisco authorized repair partner.
9. “Stolen” means any Cisco product that You have reported to the appropriate legal authorities as stolen and has likewise notified Cisco, through customer’s designated representative(s). Cisco may seek verifying information from You or law enforcement authorities as to the status of the relevant product.

10. “Unauthorized” means new or used Cisco products that are sourced and/or sold outside Cisco’s Authorized Channels network

Terms of Use

Cisco Customer Experience Cloud (CX Cloud)

These Terms of Use are part of the [General Terms](#) or similar terms existing between You and Cisco (including the End User License Agreement) (the "Agreement"). Capitalized terms, unless defined in this document, have the meaning in the Agreement. References to the Software End User License Agreement or SEULA in the Agreement mean Terms of Use.

1. Summary

Cisco Customer Experience Cloud ("CX Cloud") is a web-based portal designed to be used by Cisco customers in support of one or more Cisco products and services ("Supported Offers"). In addition to the General Terms and these Terms of Use, the Supported Offers' terms and conditions continue to apply, including the terms and conditions found in any applicable [Service Description](#) or [Offer Description](#).

2. Use of CX Cloud

2.1 Administrative Accounts. Cisco will make available one or more administrative accounts to you in CX Cloud. Users assigned administrative accounts are referred to as "Super Administrators". You authorize your Super Administrators to perform CX Cloud administrative responsibilities including, without limitation, determining whether to import or keep your data in CX Cloud, and granting, denying or limiting your users' access to CX Cloud and granting, deny or limit access to CX Cloud data to your Authorized Channel partners. You must ensure that the Super Administrators are employed by you and are appropriately qualified to act in this capacity on your behalf. You may change your Super Administrator at any time. You must not permit anyone other than your designated Super Administrators to perform any administrative activities of any kind on the CX Cloud (such as, for example, anyone acting for and on behalf of an Authorized Channel Partner). If a Super Administrator does not activate or use their account within a reasonable time period, Cisco may assign a Super Administrator on your behalf. Cisco may assign access to CX Cloud data on your behalf to our personnel, but only to the extent reasonably necessary to provide you with CX Cloud or associated services. You authorize and designate Super Administrators to receive notifications related to CX Cloud on your behalf, including without limitation, notifications related to vulnerabilities and data breaches.

2.2 Sources of Information. CX Cloud may include data gathered from other Cisco Products and Services you use to help provide you with an in-depth view of your networks and systems. This information may include System Information gathered from Data Collection Tools that you may have operating as part of a Cisco CX Service. Please see the Service Descriptions for your CX Services and the CX Cloud Privacy Data Sheet for more information.

2.3 Third Party Content. From within CX Cloud, you may choose to access certain content made available to you by third parties ("Third-Party Content"). For example, if you purchased certain CX Services, such as Success Tracks or Business Critical Services, your Authorized Channel partner may provide you with its own "Ask-the-Expert" and "Accelerator" content. If you choose to access Third-Party Content, your use of that Third-Party Content will be governed by terms between you and the third party and any questions about those terms and Third-Party Content should be addressed directly to the Third-Party Content provider. Cisco does not warrant the availability, accuracy, reliability, completeness, usefulness, non-infringement, or quality of any Third-Party Content and hereby disclaims all express and implied warranties, including any implied warranties of merchantability or fitness for a particular purpose, relating to the Third-Party Content. The Third-Party Content provider retains all right, title and interest it may have in the Third-Party Content, including all copyright and other intellectual property rights.

2.4 Product APIs. Cisco may provide you a limited license to use an Application Programming Interface with CX Cloud ("Product API"). By accessing, downloading, copying, distributing, calling, or otherwise making any use of the Product API, you accept and agree to be bound by the Cisco API License with respect to the Product API.

2.5 Other Cisco Platforms. The Product may provide you with the ability to access other Cisco platforms, dashboards and portals (“Platforms”). These Platforms will be considered separate Supported Offers for purposes of these Supplemental Terms. Each user must separately have access rights assigned to these Platforms in order to access these Platforms.

3. Data Protection

Privacy Data Sheet. The attached [Customer Experience \(CX\) Privacy Data Sheet](#) describes the Personal Data that Cisco collects and processes as part of delivering the Product.

4. Special Terms

4.1 Changes to the Product. We may enhance or change CX Cloud features at our discretion as long as we do not materially reduce your access (either in CX Cloud or elsewhere) to the core functionality we are obligated to provide as part of your Supported Offers.

4.2 Recommendations. CX Cloud may contain guidance, training, recommendations or advice (collectively, “Recommendations”), which we provide based on Cisco and industry practices as well as the information you provide to Cisco. You remain responsible for determining (i) the suitability of the Recommendations for your business, network design, regulatory compliance, security requirements, privacy and other requirements, and (ii) whether the Recommendations comply with laws applicable to your business. When making any changes based on the Recommendations, we strongly recommend you take the necessary steps to protect your network environment, including data back-ups or, if applicable, testing in a non- production environment.

4.2 Disclaimer. Except as expressly set forth as part of an Agreement with Cisco for the purchase and use of supported offerings, Cisco provides CX Cloud to you on an “AS-IS” basis without any warranties, express or implied, including warranties of merchantability and fitness for a particular purpose.

Virtual Visitation Service: Service Summary

The Cisco Virtual Visitation Service (VVS) is available as an optional service within [Solution Attached Services](#). VVS specific service elements are described in this Service Summary.

Offer Summary:

VVS provides an overlay on existing Webex meeting and Webex devices to make virtual visitation for incarcerated persons easier for correctional facilities to adopt and manage. The service allows for zero touch meeting start/end in a controlled environment and implementation of business rules within a role based scheduling portal. The service can be utilized as a process-based reservation system allowing for visits with family members, consultation with attorneys and participating in court hearings.

Cisco will deploy and host a tele visit portal to connect incarcerated individuals with providers and visitors. The service will be integrated, depending on need, to Cisco Webex, email such as Microsoft Exchange, Single Sign on using SAML and a Jail Management System. The Cisco team will work with your identified team to administratively configure a cloud-based deployment solution in alignment with your guidelines.

Implementation Summary:

Cisco and customer will participate in a Solution Design Workshop. Following the workshop, a Solution Design document encompassing the below elements, will be provided:

- Virtual Visitation Service features and functionality
- Definition of workflows
- Integration definition, if applicable
- High-level architecture diagram

VVS implementation activities will include:

- i. Set up of a Virtual Visitation Service scheduling portal.
- ii. Integrating the scheduler portal with customer's Jail Management System (JMS) via JSON file transfer method, if applicable.
- iii. Configuration of the following workflows in the scheduler portal based on customer need:
- iv. Attorney Visitation
- v. Friends and Family Visitation
- vi. Court Hearing
- vii. Brand and configure features of the scheduler portal within existing portal functionality.
- viii. Integration with Webex Control Hub
- ix. Configuration of Cisco video endpoints (DX80, Webex Desk Pro, Webex Room Kit, SX10, SX20) within the VVS platform.
- x. Functional testing.
- xi. Updating the Solution Design document to include implemented components, devices, and applications to reflect the final "as-built" design.
- xii. Knowledge transfer including a User Guide.

Assumptions:

The customer will manage the delivery, installation, configuration and updating of equipment not provided by Cisco that is required to work with, or act as, part of the Cisco-provided equipment as well as complete the following tasks within 10 Business Days of completion of the Solution Design document to allow Cisco to complete implementation activities:

- i. Ensure Cisco has access to key customer stakeholders and customer site (including physical and/or remote access to solution, devices, and facilities) as necessary for Cisco to perform implementation activities.
- ii. Provide sample data that will be provided by the customer's JMS system.
- iii. Provide access to the customer's Webex Control hub for integration.
- iv. Provide access for email integration.
- v. Provide Cisco with confirmation of the following:
 - 1) Customer's LAN and WAN is ready to support a real-time collaboration solution.
 - 2) Customer's network has enough bandwidth to support HD 720p video.
 - 3) For federated SSO requirements, ensure that the following is met: customer has an SSO system that is SAML 2.0 compliant or meets the WS Federation 1.0 standard.
- vi. Provide a corporate X.509 public key certificate to be imported into Cisco Webex SAML assertions sent to Cisco Webex signed with the certificate's private key.
- vii. Manage any customer internal change management procedures.

Support:

Cisco will provide support for VVS, including troubleshooting issues, and addressing reported service problems using reasonable commercial efforts. Support for VVS will be provided via the following mailer: vvs-support@external.cisco.com during standard business hours on business days "Standard business hours" means 9:00 a.m. to 5:00 p.m., Eastern Time; "business day" means Monday through Friday, excluding Cisco-observed holidays.

Cisco will use commercially reasonable efforts to respond the next business day to high priority issues such as scheduler outages, issues preventing business critical operations, or loss of limited but key functionality. Cisco will also provide customer access to VVS Scheduler version upgrades that may be released by Cisco from time to time. New versions may include bug fixes as well features and functionality available for existing use cases with release notes being made available with each new version.