



**CONTRACT AMENDMENT # 12
EXTENSION # 6**

This amendment by and between the Contractor and State Entity defined below shall be effective as of the date this Amendment is fully executed.

STATE OF GEORGIA CONTRACT	
State Entity's Name:	Department of Administrative Services
Contractor's Full Legal Name:	Cisco Systems, Inc.
Contract No.:	99999-SPD-T20120501-0006
Solicitation Title/Event Name:	Networking Equipment and IT Infrastructure Products
Contract Award Date:	June 21, 2012
Current Contract Term:	10/1/2020 – 2/28/2022

BACKGROUND AND PURPOSE. The Contract is in effect through the Current Term provided above. The parties hereto now desire to amend the contract to extend for an additional term of seven months and include the attached End User License Agreement.

For good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties do hereby agree as follows:

1. **CONTRACT EXTENSION.** The parties hereby agree that the contract will be extended for an additional period of time as follows:

NEW CONTRACT TERM	
Beginning Date of New Contract Term:	03/1/2022
End Date of New Contract Term:	09/30/2022


CONTRACT NUMBER: 99999-SPD-T20120501-0006

The parties agree the contract will expire at midnight on the date defined as the "End Date of the New Contract Term" unless the parties agree to extend the contract for an additional period of time.


2. **END USER LICENSE AGREEMENT.** Cisco Systems, Inc's End User License Agreement (EULA) is incorporated by reference into Statewide Contract 99999-SPD-T20120501-0006 as Attachment A to this Amendment. Any previous versions of the EULA referenced in Statewide Contract 99999-SPD-T20120501-0006 will be replaced by Attachment A to this Amendment.
3. **SUCCESSORS AND ASSIGNS.** This Amendment shall be binding upon and inure to the benefit of the successors and permitted assigns of the parties hereto.
4. **ENTIRE AGREEMENT.** Except as expressly modified by this Amendment, the contract shall be and remain in full force and effect in accordance with its terms and shall constitute the legal, valid, binding and enforceable obligations to the parties. This Amendment and the contract (including any written amendments thereto), collectively, are the complete agreement of the parties and supersede any prior agreements or representations, whether oral or written, with respect thereto. Should the State of Georgia (DOAS) enter into a new contract for these products and/or services, during the term of this Extension, the new contract shall supersede this Extension.

IN WITNESS WHEREOF, the parties have caused this Amendment to be duly executed by their authorized representatives.

CONTRACTOR

Contractor's Full Legal Name: (PLEASE TYPE OR PRINT)	Cisco Systems, Inc.
Authorized Signature:	
Printed Name and Title of Person Signing:	Jenn Pate Authorized Signatory
Date:	January 24, 2022
Company Address:	170 West Tasman Drive San Jose, CA 95134

STATE ENTITY**APPROVED BY LEGAL**

Authorized Signature:	
Printed Name and Title of Person Signing:	Jim Barnaby Deputy Commissioner – State Purchasing Division
Date:	1/31/2022
Company Address:	200 Piedmont Avenue, S.E., Suite 1302, West Tower Atlanta, Georgia 30334-9010



ATTACHMENT A

Cisco End User License Agreement

Table of Contents

Section 1. Scope and Applicability	Section 8. Warranties and Representations
Section 2. Using Cisco Technology	Section 9. Reserved
Section 3. Additional Conditions of Use	Section 10. Termination and Suspension
Section 4. Fees	Section 11. Verification
Section 5. Confidential Information and Use of Data	Section 12. General Provisions
Section 6. Ownership	Section 13. Definitions
Section 7. Reserved	

Section 1. Scope and Applicability

This End User License Agreement (“**EULA**”) between The State of Georgia and Cisco covers Your use of the Software and Cloud Services (“**Cisco Technology**”) as purchased under the State of Georgia Networking Equipment and IT Infrastructure Products #99999-SPD-T20120501-006 (“The State of Georgia Statewide Contract”). This document also incorporates any Product Specific Terms that may apply to the Cisco Technology You acquire. Definitions of capitalized terms are in Section 13 (Definitions).

You agree to be bound by the terms of this EULA through (a) Your download, installation, or use of the Cisco Technology; or (b) Your express agreement to this EULA.

If You do not have authority to enter into this EULA or You do not agree with its terms, do not use the Cisco Technology. You may request a refund for the Software within 30 days of Your initial purchase provided You return the Software to the Approved Source and disable or uninstall it. This paragraph does not apply where You have expressly agreed to end user license terms with Cisco as part of a transaction with an Approved Source.

Section 2. Using Cisco Technology

- 2.1. License and Right to Use.** Cisco grants You a non-exclusive, non-transferable (except with respect to Software as permitted under **Appendix 1**, Cisco Software Transfer and Re-Use Policy) (a) license to use the Software; and (b) right to use the Cloud Services, both as acquired from an Approved Source, for Your direct benefit during the Usage Term and as set out in Your Entitlement and this EULA (collectively, the “**Usage Rights**”).
- 2.2. Use by Third Parties.** You may permit Authorized Third Parties to exercise the Usage Rights on Your behalf, provided that You are responsible, to the extent permitted by law, for (a) ensuring that such Authorized Third Parties comply with this EULA and (b) any breach of this EULA by such Authorized Third Parties.
- 2.3. Beta and Trial Use.** If Cisco grants You Usage Rights in the applicable Cisco Technology on a trial, evaluation, beta or other free-of-charge basis (“**Evaluation Software and Services**”), You may only use the Evaluation Software and Services on a temporary basis for the period limited by the license key or specified by Cisco in writing. If there is no period identified, such use is limited to 30 days after the Evaluation Software and Services are made available to You. Cisco, in its discretion, may stop providing the Evaluation Software and Services during the trial period and/or prior to initial payment, at which point You will no longer have access to any related data, information, and files and must immediately cease using the Cisco Technology. The Evaluation Software and Services may not have been subject to Cisco’s usual testing and quality assurance processes and may contain bugs, errors, or other issues. Except where agreed to in writing by Cisco, You will not put Evaluation Software and Services into production use. Cisco provides Evaluation Software and Services “AS-IS” without support or any express or implied warranty or indemnity for any problems or issues, and Cisco will not have any liability relating to Your use of the Evaluation Software and Services.
- 2.4. Upgrades or Additional Copies of Software.** You may only use Upgrades or additional copies of the Software beyond Your license Entitlement if You have (a) acquired such rights under a support agreement covering the applicable Software; or (b) You have purchased the right to use Upgrades or additional copies separately.
- 2.5. Interoperability of Software.** If required by law and upon Your request, Cisco will provide You with the information needed to achieve interoperability between the Software and another independently created program, provided You agree to any additional terms reasonably required by Cisco. You will treat such information as Confidential Information as allowed by Georgia Open Records Act OCGA 50-18-70.
- 2.6 Subscription Renewal.** Usage Rights in Cisco Technology acquired on a subscription basis will renew for the renewal period indicated on the order You or Your Cisco Partner placed with Cisco (“**Renewal Term**”) upon written notification of intent to renew by the procuring entity, such as issuance of a Purchase Order.

Section 3. Additional Conditions of Use

- 3.1. Cisco Technology Generally.** Unless expressly agreed by Cisco, You may not (a) transfer, sell, sublicense, monetize or make the functionality of any Cisco Technology available to any third party; (b) use the Software on second hand or refurbished Cisco equipment not authorized by Cisco, or use Software that is licensed for a specific device on a different device (except as permitted under **Appendix 2**, Cisco’s Software License Portability Policy); (c) remove, modify, or conceal any product identification, copyright, proprietary, intellectual property notices or other marks; (d) reverse engineer, decompile, decrypt, disassemble, modify, or make derivative works of the Cisco Technology; or (e) use Cisco Content other than as part of Your permitted use of the Cisco Technology.
- 3.2. Cloud Services.** You will not intentionally (a) interfere with other customers’ access to, or use of, the Cloud Service, or with its security; (b) facilitate the attack or disruption of the Cloud Service, including a denial of service attack,

unauthorized access, penetration testing, crawling, or distribution of malware (including viruses, trojan horses, worms, time bombs, spyware, adware, and cancelbots); (c) cause an unusual spike or increase in Your use of the Cloud Service that negatively impacts the Cloud Service's operation; or (d) submit any information that is not contemplated in the applicable Documentation.

3.3. Data Location. Cisco shall provide You with information to enable You to procure Cisco Technology that is provided to the Authorized Entity solely from data centers in the U.S. Cisco shall provide You with information to enable You to procure Cisco Technology where storage of Customer Content data, as defined in Cisco's **Appendix 3**, Data Briefs, at rest shall be located solely in data centers in the U.S. The Contractor shall permit its personnel and contractors to access Customer Content data remotely outside of the U.S. only as required to provide technical support.

3.4. Evolving Cisco Technology. Cisco may: (a) enhance or refine a Cloud Service, although in doing so, Cisco will not materially reduce the core functionality of that Cloud Service, except as contemplated in this Section; and (b) perform scheduled maintenance of the infrastructure and software used to provide a Cloud Service, during which time You may experience some disruption to that Cloud Service. Whenever reasonably practicable, Cisco will provide You with advance notice of such maintenance. You acknowledge that, from time to time, Cisco may need to perform emergency maintenance without providing You advance notice, during which time Cisco may temporarily suspend Your access to, and use of, the Cloud Service.

Cisco may end the life of Cisco Technology, including component functionality ("EOL"), by providing written notice on <https://www.cisco.com/c/en/us/products/eos-eol-listing.html>. If You or Your Cisco Partner prepaid a fee for Your use of the Cisco Technology that becomes EOL before the expiration of Your then-current Usage Term, Cisco will use commercially reasonable efforts to transition You to a substantially similar Cisco Technology. If Cisco does not have substantially similar Cisco Technology, then Cisco will credit You or Your Cisco Partner any unused portion of the prepaid fee for the Cisco Technology that has been declared EOL ("EOL Credit"). The EOL Credit will be calculated from the last date the applicable Cisco Technology is available to the last date of the applicable Usage Term. Such credit can be applied towards the future purchase of Cisco products.

3.5. Protecting Account Access. You will keep all account information up to date, use reasonable means to protect Your account information, passwords and other login credentials, and promptly notify Cisco of any known or suspected unauthorized use of or access to Your account.

3.6. Use with Third-Party Products. If You use the Cisco Technology together with third-party products, such use is at Your risk. You are responsible for complying with any third-party provider terms, including its privacy policy. Cisco does not provide support or guarantee ongoing integration support for products that are not a native part of the Cisco Technology.

3.7. Open Source Software. Open source software not owned by Cisco is subject to separate license terms as set out at www.cisco.com/go/opensource. The applicable open source software licences will not materially or adversely affect Your ability to exercise Usage Rights in applicable Cisco Technology.

Section 4. Fees

To the extent permitted by law, orders for the Cisco Technology are non-cancellable. Fees for Your use of Cisco Technology are set out in Your purchase terms with Your Approved Source. If You use Cisco Technology beyond Your Entitlement ("**Overage**"), the Approved Source may invoice You, and You agree to pay, for such Overage.

Section 5. Confidential Information and Use of Data

- 5.1. Confidentiality.** Recipient will hold in confidence and use no less than reasonable care to avoid disclosure of any Confidential Information to any third party, except for its employees, affiliates, and contractors who have a need to know (“**Permitted Recipients**”). Recipient: (a) must ensure that its Permitted Recipients are subject to written confidentiality obligations no less restrictive than the Recipient’s obligations under this EULA, and (b) is liable for any breach of this Section by its Permitted Recipients. Such nondisclosure obligations will not apply to information that: (i) is known by Recipient without confidentiality obligations; (ii) is or has become public knowledge through no fault of Recipient; or (iii) is independently developed by Recipient. Recipient may disclose Discloser’s Confidential Information if required under a regulation, law or court order provided that Recipient provides prior notice to Discloser (to the extent legally permissible) and reasonably cooperates, at Discloser’s expense, regarding protective actions pursued by Discloser. Upon the reasonable request of Discloser, Recipient will either return, delete or destroy all Confidential Information of Discloser and certify the same.
- 5.2. How We Use Data.** Cisco will access, process and use data in connection with Your use of the Cisco Technology in accordance with applicable privacy and data protection laws. For further detail, please visit **Appendix 3**, Cisco’s Data Briefs.
- 5.3. Notice and Consent.** To the extent Your use of the Cisco Technology requires it, You are responsible for providing notice to, and obtaining consents from, individuals regarding the collection, processing, transfer and storage of their data through Your use of the Cisco Technology.

Section 6. Ownership

Except where agreed in writing, nothing in this EULA transfers ownership in, or grants any license to, any intellectual property rights. You retain any ownership of Your content and Cisco retains ownership of the Cisco Technology and Cisco Content. Cisco may use any feedback You provide in connection with Your use of the Cisco Technology as part of its business operations.

Section 7. ReservedSection 8. Warranties and Representations

- 8.1. Performance.** Cisco warrants that: (a) for a period of 90 days from the Delivery Date or longer as stated in Documentation, or in Section J, Warranties in Attachment 1 to the State of Georgia Statewide Contract the Software substantially complies with the Documentation; and (b) during the Usage Term, it provides the Cloud Services with commercially reasonable skill and care in accordance with the Documentation and Product Specific Terms.
- 8.2. Malicious Code.** Cisco will use commercially reasonable efforts to deliver the Cisco Technology free of Malicious Code.
- 8.3. Qualifications.** Sections 8.1 and 8.2 do not apply if the Cisco Technology or the equipment on which it is authorized for use: (a) has been altered, except by Cisco or its authorized representative; (b) has been subjected to abnormal

physical conditions, accident or negligence, or installation or use inconsistent with this EULA or Cisco's instructions; (c) is acquired on a no charge, beta or evaluation basis; (d) is not a Cisco-branded product or service; or (e) has not been provided by an Approved Source. Upon Your prompt written notification to the Approved Source during the warranty period of Cisco's breach of this Section 8, Your sole and exclusive remedy (unless otherwise required by applicable law) is, at Cisco's option, either (i) repair or replacement of the applicable Cisco Technology or (ii) a refund of the (a) license fees paid or due for the non-conforming Software, or (b) the fees paid for the period in which the Cloud Service did not comply, excluding any amounts paid under a service level agreement/objective, if applicable.

Where Cisco provides a refund of license fees paid for Software, You must return or destroy all copies of the applicable Software. **Except as expressly stated in this Section, to the extent allowed by applicable law, Cisco expressly disclaims all warranties and conditions of any kind, express or implied, including without limitation any warranty, condition or other implied term as to merchantability, fitness for a particular purpose or non-infringement, or that the Cisco Technology will be secure, uninterrupted or error free.** If You are a consumer, You may have legal rights in Your country of residence that prohibit the limitations set out in this Section from applying to You, and, where prohibited, they will not apply.

Section 9. Reserved

Section 10. Termination and Suspension

- 10.1. Suspension.** Cisco may immediately suspend Your Usage Rights if You breach Sections 2.1 (License and Right to Use), 3.1 (Cisco Technology Generally), 3.2 (Cloud Services) or 12.8 (Export).
- 10.2. Termination.** If a party materially breaches this EULA and does not cure that breach within 30 days after receipt of written notice of the breach, the non-breaching party may terminate this EULA for cause. Cisco may immediately terminate this EULA if You breach Sections 2.1 (License and Right to Use), 3.1 (Cisco Technology Generally), 3.2 (Cloud Services) or 12.8 (Export). Upon termination of the EULA, You must stop using the Cisco Technology and destroy any copies of Software and Confidential Information within Your control. If this EULA is terminated due to Cisco's material breach, Cisco will refund You or Your Approved Source, the prorated portion of fees You have prepaid for the Usage Rights beyond the date of termination. Upon Cisco's termination of this EULA for Your material breach, You will pay Cisco or the Approved Source any unpaid fees through to the end of the then-current Usage Term. If You continue to use or access any Cisco Technology after termination, Cisco or the Approved Source may invoice You, and You agree to pay, for such continued use.

Section 11. Verification

During the Usage Term and for a period of 12 months after its expiry or termination, You will take reasonable steps to maintain complete and accurate records of Your use of the Cisco Technology sufficient to verify compliance with this EULA ("**Verification Records**"). Upon reasonable advance notice, and no more than once per 12 month period, You will, within 30 days from Cisco's notice, allow Cisco and its auditors access to the Verification Records and any applicable books, systems (including Cisco product(s) or other equipment), and accounts during Your normal business hours. If the verification process discloses underpayment of fees: (a) You will pay such fees; and (b) Auditor will not be paid additional fees based upon the findings of the audit. For the purposes of clarification, You will provide evidence related to any of the below applicable scenarios where You may have the right to run Products.

- for trial or try and buy
- acquired by or through a third party
- for testing
- in preparation for equipment/device decommission
- on device/equipment no longer in production

Section 12. General Provisions

- 12.1 Survival.** Sections 4, 5, 6, 8, 10, 11 and 12 survive termination or expiration of this EULA.
- 12.2 Third-Party Beneficiaries.** This EULA does not grant any right or cause of action to any third party.
- 12.3 Assignment and Subcontracting.** Except as set out below, neither party may assign or novate this EULA in whole or in part without the other party's express written consent. Cisco may (a) by written notice to You, assign or novate this EULA in whole or in part to an Affiliate of Cisco, or otherwise as part of a sale or transfer of any part of its business; or (b) subcontract any performance associated with the Cisco Technology to third parties, provided that such subcontract does not relieve Cisco of any of its obligations under this EULA.

- 12.4 U.S. Government End Users.** The Software, Cloud Services and Documentation are deemed to be “commercial computer software” and “commercial computer software documentation” pursuant to FAR 12.212 and DFARS 227.7202. All U.S. Government end users acquire the Software, Cloud Services and Documentation with only those rights set forth in this EULA. Any provisions that are inconsistent with federal procurement regulations are not enforceable against the U.S. Government.
- 12.5 Cisco Partner Transactions.** If You purchase Cisco Technology from a Cisco Partner, the terms of this EULA apply to Your use of that Cisco Technology and prevail over any inconsistent provisions in Your agreement with the Cisco Partner.
- 12.6 Compliance with Laws.** Each party will comply with all laws and regulations applicable to their respective obligations under this EULA. Cisco may restrict the availability of the Cisco Technology in any particular location or modify or discontinue features to comply with applicable laws and regulations.
- If You use the Cisco Technology in a location with local laws requiring a designated entity to be responsible for collection of data about individual end users and transfer of data outside of that jurisdiction (e.g. Russia and China), You acknowledge that You are the entity responsible for complying with such laws.
- 12.7 Export.** Cisco’s Software, Cloud Services, products, technology and services (collectively the “Cisco Products”) are subject to U.S. and local export control and sanctions laws. You acknowledge and agree to the applicability of and Your compliance with those laws, and You will not receive, use, transfer, export or re-export any Cisco Products in a way that would cause Cisco to violate those laws. You also agree to obtain any required licenses or authorizations.
- 12.8 Governing Law and Venue.** This EULA, and any disputes arising from it, will be governed exclusively by the applicable governing law below, based on Your primary place of business and without regard to conflicts of laws rules or the United Nations Convention on the International Sale of Goods. The courts located in the applicable venue below will have exclusive jurisdiction to adjudicate any dispute arising out of or relating to the EULA or its formation, interpretation or enforcement. Each party hereby consents and submits to the exclusive jurisdiction of such courts. Regardless of the below governing law, either party may seek interim injunctive relief in any court of appropriate jurisdiction with respect to any alleged breach of Cisco’s intellectual property or proprietary rights.

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

If You are a United States public sector agency or government institution located in the United States, the laws of the primary jurisdiction in which You are located will govern the EULA and any disputes arising from it. For U.S. Federal Government customers, this EULA will be controlled and construed under the laws of the United States of America.

- 12.9 Notice.** Any notice delivered by Cisco to You under this EULA will be delivered via email, regular mail or postings on Cisco.com depending on the type of notice that is being provided. Where applicable and feasible, notice shall be provided to the then current Contract Manager or as agreed to under Section L, 17 Notices in Attachment 1, to the State of Georgia Statewide Contract. Notices to Cisco should be sent to Cisco Systems, Office of General Counsel, 170 Tasman Drive, San Jose, CA 95134 unless this EULA, applicable Product Specific Terms or an order specifically allows other means of notice.
- 12.10 Force Majeure.** Except for payment obligations, neither party will be responsible for failure to perform its obligations due to an event or circumstances beyond its reasonable control.
- 12.11 No Waiver.** Failure by either party to enforce any right under this EULA will not waive that right.
- 12.12 Severability.** If any portion of this EULA is not enforceable, it will not affect any other terms.
- 12.13 Entire agreement.** This EULA is the complete agreement between the parties with respect to the subject matter of this EULA and supersedes all prior or contemporaneous communications, understandings or agreements (whether

written or oral).

12.14 Translations. Cisco may provide local language translations of this EULA in some locations. You agree that those translations are provided for informational purposes only and if there is any inconsistency, the English version of this EULA will prevail.

12.15 Order of Precedence. If there is any conflict between this EULA and any Product Specific Terms expressly referenced in this EULA, the order of precedence is: (a) such Product Specific Terms; (b) this EULA (excluding the Product Specific Terms and any Cisco policies); then (c) any applicable Cisco policy expressly referenced in this EULA.

Section 13. Definitions

“Affiliate” 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 more than 50% of the relevant party; or (b) be able to direct the affairs of the relevant party through any lawful means (e.g., a contract that allows control).

“Approved Source” means Cisco or a Cisco Partner.

“Authorized Third Parties” means Your Users, Your Affiliates, Your third-party service providers, and each of their respective Users permitted to access and use the Cisco Technology on Your behalf as part of Your Entitlement.

“Cisco” “we” “our” or “us” means Cisco Systems, Inc. or its applicable Affiliate(s).

“Cisco Content” means any (a) content or data provided by Cisco to You as part of Your use of the Cisco Technology and (a) content or data that the Cisco Technology generates or derives in connection with Your use. Cisco Content includes geographic and domain information, rules, signatures, threat intelligence and data feeds and Cisco’s compilation of suspicious URLs.

“Cisco Partner” means a Cisco authorized reseller, distributor or systems integrator authorized by Cisco to sell Cisco Technology.

“Cloud Service” means the Cisco hosted software-as-a-service offering or other Cisco cloud-enabled feature described in the applicable Product Specific Terms. Cloud Service includes applicable Documentation and may also include Software.

“Confidential Information” means non-public proprietary information of the disclosing party (**“Discloser”**) obtained by the receiving party (**“Recipient”**) in connection with this EULA, which is (a) conspicuously marked as confidential or, if verbally disclosed, is summarized in writing to the Recipient within 14 days and marked as confidential; or (b) is information which by its nature should reasonably be considered confidential whether disclosed in writing or verbally.

“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.

“Delivery Date” means the date agreed in Your Entitlement, or where no date is agreed: (a) where Usage Rights in Software or Cloud Services are granted separately: (i) for Software, the earlier of the date Software is made available for download or installation, or the date that Cisco ships the tangible media containing the Software, and (ii) for Cloud Services, the date on which the Cloud Service is made available for Your use; or (b) where Usage Rights in Software and Cloud Services are granted together, the earlier of the date Software is made available for download, or the date on which the Cloud Service is made available for Your use.

“Documentation” means the technical specifications and usage materials officially published by Cisco specifying the functionalities and capabilities of the applicable Cisco Technology.

“Entitlement” means the specific metrics, duration, and quantity of Cisco Technology that You commit to acquire from an Approved Source through individual acquisitions or Your participation in a Cisco buying program.

“Malicious Code” means code that is 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 Technology (for example, as part of some of Cisco’s security products).

“Product Specific Terms” means additional product related terms applicable to the Cisco Technology You acquire as set out at www.cisco.com/go/softwareterms.

“Software” means the Cisco computer programs including Upgrades, firmware and applicable Documentation.

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

“Usage Term” means the period commencing on the Delivery Date and continuing until expiration or termination of the

Entitlement, during which period You have the right to use the applicable Cisco Technology.

“**User**” means the individuals (including contractors or employees) permitted to access and use the Cisco Technology on Your behalf as part of Your Entitlement.

“**You**” means the individual or legal entity purchasing the Cisco Technology.



APPENDIX 1

Software License Transfer and Re-Use Policy

Purpose

This document sets forth Cisco's policy regarding the transfer of Cisco Software licenses (the "Policy"). An authorized transfer occurs when the licensee conveys or assigns the Software license to another entity after receipt of Cisco's consent and payment of any applicable license fee or any other conditions required by Cisco. Use of Cisco Software by the transferee is governed by the then-current Cisco End User License Agreement ("EULA") available at www.cisco.com/go/softwareterms.

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:

"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.

Transfer Policy

Unless prohibited by applicable law or expressly allowed by Cisco in the applicable license terms or otherwise provided below, Software is not transferable until and unless: (1) Cisco approves the Software Transfer Request Form referenced herein *and* (2) you pay any applicable license fees, including payment of all outstanding license fees invoiced and paid periodically. The transferee also may be required to pay service inspection or reinstatement fees in accordance with [Cisco policies](#) before any transfer is permitted.

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 shall 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 shall be subject to payment of Cisco's then-current applicable software relicensing fee and shall be 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 are 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.

Exceptions

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 valid licensee (“Licensee” or “Transferor”) without payment of the license fee, provided that the Conditions of Any Transfer terms (set forth below) are met.

1. **Affiliate:** A Licensee 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 Licensee; (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.
2. **Merger, Acquisition or Divestiture:** In the event the Licensee is wholly acquired or merges its business with another entity or the Licensee 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, the Licensee may transfer its right to use the Software to the acquiring or divested entity.
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 Any Transfer and the payment of the applicable license fee.
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 at the end user’s premises.
 - a. Original End User. The managed service provider (“Licensee” in this paragraph 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 (12) 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.

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:
- 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;
 - The Software must be used only for Government End User's internal use; and,
 - 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.

6. **Outsourcing by Original End User Licensee:** If the original end user ("Licensee" in this paragraph 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.
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 located in Europe ("Transferee") 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.

Conditions of Transfer

Transfers shall only be allowed under the following conditions:

- Neither party involved in the transfer is in breach of any agreements with Cisco and/or governing the use of the Software.
- 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.

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.
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. Both authorized parties to the transfer complete and submit the [Software License Transfer Request Form](#) and comply with its requirements.

Re-Use Policy

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 shall 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 (eg 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.
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.

Questions?

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



APPENDIX 2

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 non-Cisco 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/one-software/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.

APPENDIX 3 – DATA BRIEFS

[Systems Information, Customer Content, Personal Data data briefs follow]

Systems Information

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 customer-focused 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	<p>Data generated by instrumentation and logging systems created through the use and operation of the product or service.</p> <p>Examples:</p> <ul style="list-style-type: none"> • <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	<ul style="list-style-type: none"> • 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. <p>Solution integration to customer business and IT processes.</p>
Accelerate Adoption	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Product innovation, software updates, development of new features and offers, threat intelligence detection improvements. • Serviceability and product quality improvements aligned to customer satisfaction.

Personal Data

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 Master Data Protection Agreement

When Cisco is acting as data processor (i.e. managing Personal Data on behalf of our customers), our Master Data Protection Agreement (MDPA), 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 MDPA is publicly available on the Cisco Trust Center ([here](#)). Key elements in the MDPA 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 MDPA, 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 MDPA [here](#).

Customer Content

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.

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. 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](#).

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 Teams rooms content