Cisco General Disclosures

1. General Disclosures for Cisco Offers

These General Disclosures describe how Cisco handles data across Cisco Offers and replace the Data Briefs previously published on the Cisco Trust Center and Cisco Trust Portal. Capitalized words not otherwise defined in these General Disclosures have the meanings set forth in the Cisco General Terms. Cisco Offer Disclosures contain information specific to an applicable Cisco Offer, which can be found on the Cisco Trust Portal and take precedence over these General Disclosures. If there is a difference in the translated, non-English versions of this document, the US-English version will take precedence.

2. Data Types and Handling

Cisco classifies data for Cisco Offers into four categories: (1) Customer Systems Information, (2) Customer Content, (3) Cisco System Information, and (4) Cisco Content. These four categories are defined below.

Cisco recognizes data included in any of the above categories may be considered Personal Data when associated with or related to an identified or identifiable individual. If Personal Data is included or received, Cisco will treat that data as you would expect – as Personal Data – and always in accordance with applicable law, Cisco's Privacy Statement, and your agreements with us. Please see Personal Data Handling below for more details.

Customer Systems Information

Customer Systems Information is data and metadata that are unique to you and generated or collected based on your use of a Cisco Offer. Customer Systems Information can be generated or collected by a Cisco Offer or data collection tools that you have authorized.

Examples of Customer Systems Information include:

- Data generated by your use of sensors, devices, or machinery
- Data about your network usage, traffic density, and patterns
- Data about hardware and software generated when you submit a support request, and certain additional information you submit to Cisco about your issue (this excludes feedback you share with Cisco, such as comments, survey responses, product evaluations or other qualitative input, which is classified as Cisco Systems Information)
- Event data (e.g., incidents) generated by a Cisco Offer based on your configuration and policies

Customer Content

Customer Content is (i) content and digital assets that you provide to Cisco when using a Cisco Offer, (ii) content and digital assets unique to you generated from your use of a Cisco Offer, or (iii) data provided by you or on your behalf for ingestion into a data analytics platform in a Cisco Offer.

Examples of Customer Content include:

- Files you upload to a Cisco Offer that contain text, audio, video, or images
- Your Webex Meetings recordings
- Cisco and Meraki Smart Camera video recordings of your environment
- Content you provide to Cisco during a professional services engagement
- Your Webex App Spaces content

Cisco Systems Information

Cisco Systems Information is data and metadata about infrastructure, platforms, interfaces, or other components that are generated or collected by Cisco through the operation or delivery of the Cisco Offer.

Examples of Cisco Systems Information include:

- Log files or data collected about the underlying infrastructure used to operate or secure a Cisco Offer
- Feedback Cisco collects from you
- Performance, usage, and deployment topology and telemetry data collected about the operation and use of a Cisco Offer

Cisco Content

Cisco Content is digital assets, data, metadata, and other content Cisco provides as part of access to Cisco Offers.

Examples of Cisco Content include:

- Cisco Offer Documentation
- Models provided by Cisco for your use with a Cisco Offer
- Threat intelligence

Cisco uses Customer Systems Information and Customer Content as described in the table below. Cisco uses Cisco Systems Information and Cisco Content for Cisco Offer delivery, modification, and development, customer success, marketing, and for other business purposes consistent with our operational goals and objectives.

Table 1: How Cisco Uses Customer Content & Customer Systems Information

The following purposes form the basis of how and when Cisco uses Customer Content and Customer Systems Information, subject to sections 3 and 4 of these General Disclosures.

Purpose	Example
Offer Delivery	Cisco uses Customer Systems Information and Customer Content to deliver Cisco Offers. Examples include: · Providing and operating Cisco Offers · Billing, license enforcement and enablement, warranty coverage, and managing our relationship · Monitoring performance, integrity, and stability of Cisco Offers · Optimizing and securing Cisco Offers
Offer Modification	Cisco uses Customer Systems Information and Customer Content to evolve and improve the Cisco Offer(s) from which it originated. Examples include: · Correcting errors · Resolving interoperability issues · Patching security vulnerabilities · Making feature modifications, improvements, and additions · Improving services associated with Cisco Offer(s) · Security Purposes, as defined in and subject to section 3 below
New Offer Development	Cisco uses Customer Systems Information and Customer Content to innovate and develop Cisco Offers, always prioritizing customer privacy and security. Examples include: · Using device configurations and log files to identify potential issues, then creating a network performance optimization offer · Using telemetry from one Cisco Offer to recognize patterns that allow us to improve the performance of another Cisco Offer · Security Purposes, as defined in and subject to section 3 below Cisco only uses Customer Content for this purpose if we provide you notice and the ability to control whether your data is used. Cisco only uses Customer Systems Information to develop new Offers if we provide you notice and the ability to control whether your data is used or after de-identifying the dataset.
Customer Success	Cisco uses Customer Systems Information and Customer Content to help you get full value out of your purchase, achieve your business objectives, and optimize your use of Cisco Offers. Examples include: · Providing you with recommendations on how best to maximize your use of Cisco Offer(s) · Highlighting unused entitlements, capabilities, and/or features · Improving customer engagement and interactions

Marketing	Cisco uses Customer Systems Information to identify Cisco Offers you may be interested in to improve your workflows, increase operational efficiency, and address business needs. For example, using Customer Systems Information to identify a Cisco Offer that may complement or enhance your use of an existing Cisco Offer. Cisco does not use Customer Content for marketing purposes without your authorization.

Cisco may also use Customer Content and Customer Systems Information to derive analytics and insights after either de-identifying it or providing you with notice and the ability to control whether your data is used.

As used in these General Disclosures, de-identification means transforming data so that it is significantly more difficult or impossible to link the data to specific individuals or organizations. The goal is to protect individuals' and organizational rights and interests while retaining data utility for its intended purpose.

Personal Data Handling

Roles. Cisco treats Personal Data in accordance with the Cisco Privacy Statement. In jurisdictions that distinguish between data controllers and data processors, Cisco is the data controller for Personal Data processed to administer, manage, and improve the customer relationship and service. Cisco is the data processor for Personal Data processed by the Cisco Offer solely to provide the Cisco Offer's functionality.

Cross Border Data Transfer. Cisco is committed to legal, responsible international transfers.

- For EU and UK Personal Data transfers where Cisco acts as a controller, Cisco has approved Binding Corporate Rules with the Dutch Autoriteit Persoonsgegevens as its lead authority (Cisco's EU main establishment is in the Netherlands) and the UK.
- For EU, UK, and Swiss Personal Data transfers to the US, Cisco complies with the EU-US, UK Extension, and Swiss-US Data Privacy Framework.
- Cisco is also certified under the Global Cross Border Privacy Rules system and Privacy Recognition for Processors.
- For jurisdictions where Personal Data is transferred across borders and standard contractual clauses (SCCs) are available, Cisco also enters into SCCs with customers. Please refer to Cisco's Data Protection Agreement Portal for more information.

Data Subject Rights. Individuals can request their Personal Data, lodge a complaint, or exercise their privacy rights by submitting an online privacy request using this form. For more information, please review the Cisco Privacy Statement.

For more detailed information regarding Personal Data processing when using Cisco Offers, please refer to the Cisco Trust Portal for Cisco Offer Disclosures.

Sharing Customer Content and Customer Systems Information

To perform the activities described in these General Disclosures or a Cisco Offer Disclosure, Cisco may need to share Customer Content and Customer Systems Information with third parties, as described in more detail below and in the applicable Cisco Offer Disclosure.

Partners & Suppliers. Cisco may share Customer Systems Information with our trusted ecosystem of suppliers, partners, distributors, and contractors. For example, if you purchase a Cisco Offer through a Cisco partner, Cisco may provide your partner or its distributor with the Customer Systems Information needed to deliver and perform the solution, manage your subscription, and fulfill administrative activities, consistent with the purposes described above. There are also limited reasons for sharing Customer Content. For example, if a Cisco Offer 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.

In each instance, each participant in our trusted ecosystem has agreed to confidentiality terms, compliance with applicable law, and adherence to information security, privacy, and other data processing requirements with Cisco that are consistent with Cisco's commitments to you.

Research Partners. Cisco may share and use Customer Systems Information and Customer Content with trusted universities, industry groups, and external researchers to derive insights or knowledge relevant to a specific research question or objective. For example, Cisco may provide data derived from Customer Systems Information to improve threat detection, create preventative security intelligence, engage in industry insights research, or strategic research initiatives. Cisco de-identifies Customer Systems Information and Customer Content before any sharing of this type to prevent links back to specific customer(s).

Integrations. You may choose to integrate Cisco Offers with other Cisco Offers and third-party products. If you choose to integrate, or use a Cisco-provided integration for, a Cisco Offer with a third-party product, Cisco is not responsible for Customer Systems Information or Customer Content processed by you or the third party once it leaves Cisco's systems; such processing is governed by the contracts and policies between you and the third party. When you use multiple Cisco Offers together, purposes of processing, retention periods, storage location, and data collected and processed may differ between each Cisco Offer. Please review each applicable Cisco Offer Disclosure for more information.

3. Information Security

Cisco uses information security best practices and controls including policies and standards (such as our Data Protection Standard) to protect and govern Customer Content and Customer Systems Information in our possession.

Cisco security teams, such as Cisco's Security & Trust Organization and Cisco Talos, may process Customer Systems Information and Customer Content for both proactive and reactive measures to enhance the security of Cisco Offers. These measures may include researching security issues, testing Cisco Offers based on that research, and conducting Offer Modification and New Offer Development (collectively, "Security Purposes"), provided that Cisco will not design the resulting Offers (or modifications to existing Offers) to include the underlying Customer Systems Information, Customer Content, or data that can identify an individual. As part of the Security Purposes, Cisco may also Train and Fine-Tune Generative AI models (each term as defined in Section 4 below), but it will not design any resulting Offers (or modifications to existing Offers) to include the underlying Customer Systems Information, Customer Content, or data that can identify an individual.

The Cisco Security Center details how to report suspected security incidents and request support. Cisco's vulnerability management policies are also available as resources on the Cisco Security Center. If you have questions or concerns about any Cisco Offer or security notifications, contact your Cisco sales representative.

For further information about how Cisco Offers protect, use, and share data responsibly, including compliance with applicable laws, data breach notification, secure development lifecycle, data storage, and our data protection requirements, please see Cisco Offer Disclosures, our Information Security Exhibit, and Cisco Security Center.

4. Artificial Intelligence (AI)

Responsible AI

Cisco provides and deploys AI capabilities in Cisco Offers in line with our Cisco Principles for Responsible AI – transparency, fairness, accountability, privacy, security, and reliability. Cisco implements these principles by design through the Cisco Responsible AI Framework. Before Cisco provides, integrates, or deploys AI as part of a Cisco Offer, we perform an AI Impact Assessment on that use of AI, including assessing the underlying models and comparing the technical underpinnings of the capability against the Principles and Framework.

Types of Models in Cisco Offers

Cisco uses a wide range of AI models–including predictive, diagnostic, and generative models–to deliver Offers for customers. Predictive and diagnostic models typically analyze existing data to forecast trends and identify issues, usually operating within well-defined parameters. Generative AI models typically produce new output or responses based on input. For example, generative models power AI assistants that respond to customer questions by producing tailored answers.

Testing, Monitoring, and Safety

Cisco monitors and tests its AI capabilities and associated models over the course of their lifecycles. We implement robust safeguards that combine our internal measures with those of our model providers.

- **Performance Metrics**: We assess performance using relevant metrics, which may include accuracy, reliability, robustness, latency, output quality, coherence, creativity, relevance, fairness, and user satisfaction (derived from feedback). The metrics we use vary based on the model type and intended application.
- **Testing Methodologies**: Examples of testing processes include functional testing, performance testing, robustness testing, red teaming, and evaluation for potential biases. Specific testing practices vary depending on the Offer and model type.
- **Human Oversight**: Human oversight is an integral part of our AI development, deployment, and evaluation process. User feedback is a key input into this process. In the post-training phase, we may use techniques such as reinforcement learning from human feedback (RLHF) to further refine model behavior, ensuring outputs align with human preferences and the Cisco Principles for Responsible AI.
- **Ongoing Monitoring**: Cisco monitors AI features deployed in its Offers to track performance and identify areas for improvement or re-evaluation.

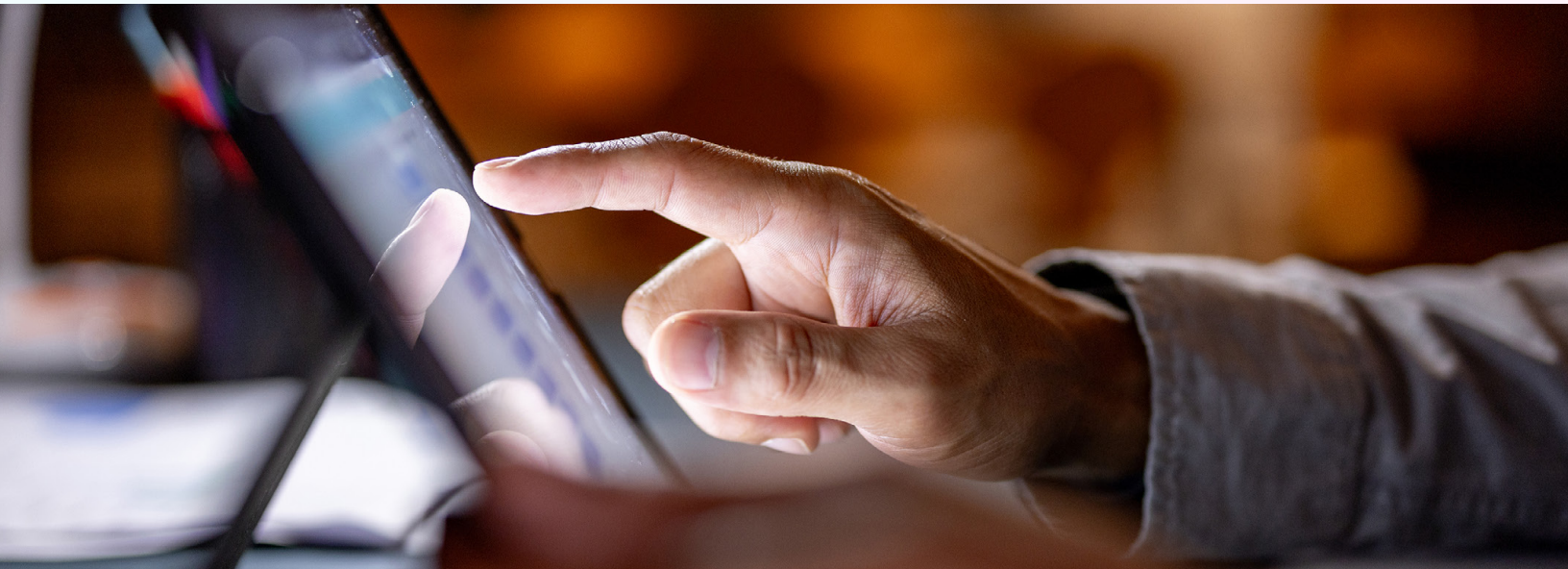
Generative Artificial Intelligence

"Generative AI" means a subset of artificial intelligence that uses specific generative technologies, including but not limited to large language models (LLMs), generative adversarial networks (GANs), and diffusion models, to produce content such as text, images, audio, or video in response to input, based on patterns learned from training data. This definition excludes general machine learning algorithms and deep learning models that do not include generative technologies. "Train and Fine-Tune" means teaching a Generative AI model how to learn patterns and perform specific tasks by supplying it with datasets and optimizing its parameters, including adapting a pre-trained Generative AI model to improve performance through methods such as adjusting its weights.

Cisco may process Customer Content and Customer Systems Information using Generative AI for the purposes stated in Table 1 above. Except for the Security Purposes stated in section 3 above and where stated in an Offer Disclosure, Cisco will only Train and Fine-Tune a Generative AI model using:

- **Customer Content** if (i) we provide notice and the ability to control whether your data is used or (ii) you select an available customer-specific model (i.e., only used by your organization).
- **Customer Systems Information** if (i) we provide notice and the ability to control whether your data is used, (ii) we de-identify the dataset, or (iii) you select an available customer-specific model.

Cisco provides details about its Generative AI-based features and Offers through Documentation and Disclosure Documents, and we make it clear to users when they are interacting with Generative AI features within a Cisco Offer's user interface. For example, our Offers generally identify outputs generated by AI, provide channels for user feedback (e.g., thumbs up/down ratings on Generative AI responses), and/or have specific controls and options governing use of Customer Systems Information and Customer Content with Generative AI. See the applicable Offer Documentation for more information.




CISCO