Supplemental Terms

Data Access Terms

These Data Access Terms (the "**Data Access Terms**") are Supplemental Terms that form part of the General Terms or similar terms existing between You and Cisco (the "**Agreement**"). Capitalized terms, unless defined in this document, have the meaning in the General Terms or Applicable Law, including the Data Act.

1. Scope and Applicability

The Data Access Terms govern the access to and use of Requested Data. By accessing Requested Data, You accept and agree that any access and use of Requested Data will be in accordance with these Data Access Terms.

2. Data Access

2.1 **Representations/Warranties.** You represent and warrant that You are either the owner of the Connected Product or are contractually entitled to use the Connected Product under the Agreement or to receive the Related Service(s) under the Agreement.

2.2 **Data Access Methods**

(A) Direct Data Access. Some Cisco Offers (as described in more detail in the Disclosure Documents) permit You to access Requested Data directly from the Cisco Offer via a Cisco API, other in-product features, or both. If You or Your Authorized Users use a Cisco API to access the Requested Data, the API License Terms and Conditions in Exhibit A attached, along with any additional terms specific to the Cisco Offer's API, govern Your access and use of the Cisco API.

(B) Data Access Upon Request. Where the Requested Data cannot be accessed directly via an Access Method, You may submit a request to ask_data@cisco.com. Cisco will provide the Requested Data to You without undue delay, free of charge, and in a structured, commonly used, and machine-readable format, in accordance with Article 4(1) of the Data Act.

(C) Where technically feasible, Cisco will provide the Requested Data continuously and in real time, via Cisco's systems. Upon written notification to Cisco, You may designate a third-party recipient (per Article 5 Data Act) and pursuant to Section 8 below (Third Party Data Access) Cisco will transmit the Requested Data to that third party under the same conditions. If direct electronic delivery is unavailable, Cisco will provide an alternative delivery mechanism (e.g., secure file download or encrypted transfer).

2.3 **Conditions of Access**

(A) Data Access and Use Restrictions

(1) You may only access and use Requested Data for the Cisco Offer for which You hold entitlements and in accordance with Applicable Laws.

(2) If You request Personal Data and are not the Data Subject, You must have a legal right to process any Personal Data included in the Requested Data.

(3) You may not access any application, system, service, computer, data, account, or network without an appropriate entitlement or prior authorization from Cisco.

(4) The underlying Cisco Offer is licensed as described in the Agreement.

(B) Credential and Access Management

(1) Your credentials (e.g., passwords, keys, and client IDs) must be kept confidential.

(2) Credentials may only be used by You and Your Authorized Users, and solely to identify applications permitted to use the Access Method.

(3) You and Your Authorized Users may use and access the Access Method only as specified in the applicable documentation (e.g. documentation for the Cisco Offer or Cisco API).

(C) Security and Integrity

(1) You may not use the Access Method to or take other actions that disable, disrupt, circumvent, interfere with, or otherwise violate the security of any Cisco product, service, network, infrastructure, or user, or any mechanism that limits or controls use of the Access Method.

(2) You are not permitted to access, use, or share Requested Data if such access, use, or sharing could: (a) bypass or disrupt any security controls or license-enforcement features of any Cisco Offer, or (b) harm or interfere with the security or performance of any Cisco product, service, or other network services, for example by carrying out denial-of-service attacks, conducting penetration testing, or distributing malware.

(3) You may not use coercive means to obtain access to Requested Data or subvert implemented processes or controls in the Data Holder's technical infrastructure that are designed to protect the Requested Data.

(4) You may not use an Access Method in a way that could create an unreasonable security or privacy risk.

(5) You may not use an unreasonable amount of bandwidth or adversely impact the stability of an Access Method or the behavior of other applications relying on it.

(D) Competition and Commercial Restrictions

(1) You may not use Requested Data to develop a product that competes with the Cisco Offer from which the Requested Data originates, nor share the Requested Data with a third party with that intent.

(2) You may not share the Requested Data with a third party considered as a gatekeeper under Article 3 of Regulation (EU) 2022/1925.

(3) You may not use the Requested Data to derive insights about the economic situation, assets, or production methods of Cisco.

(E) Compliance and Review

(1) Failure to comply with any part of these Data Access Terms constitutes a material breach of these terms.

(2) Cisco reserves the right to review Your (and Your Authorized Users') use of the Access Method.

(F) Prohibited Conduct

(1) You may not use an Access Method or Requested Data to facilitate or promote illegal activities, breach any Cisco terms and conditions, commit fraud, engage in false or misleading conduct or infringe upon the rights of any third party.

(2) You may not reverse engineer or extract source code, except as expressly permitted by Applicable Laws.

(3) You may not merge, integrate, or use any software that requires Cisco confidential information to be licensed or shared with any third party (e.g., under the GNU General Public License).

(4) You may use any Access Method in applications or situations where its failure could lead to death, serious bodily injury, or severe physical or environmental damage.

3. Protection of Trade Secrets

Cisco will identify any data that qualifies as trade secrets under Directive (EU) 2016/943 in the respective Cisco Offer Disclosure Document. If the Requested Data includes trade secret data, Cisco will only provide You with access to the trade secret data if there are appropriate confidentiality safeguards in place. Examples of such safeguards include Your executing an additional non-disclosure agreement, implementing certain access control mechanisms or technical protection measures, or ensuring Cisco access and audit rights to Your access logs to Requested Data for at least two years following the share of Requested Data with You.

When Requested Data includes trade secret data, Cisco will only provide You with access to the trade secret data if, upon receipt, You apply access controls preventing access to the trade secret data by third parties, except as allowed in section 8 (Third Party Data Access), and You limit access to those who need to know within Your business.

In accordance with the Data Act, Cisco may suspend or refuse to provide You with access to trade secret data where: (i) such safeguards are not contractually agreed or implemented, or (ii) Cisco can demonstrate that disclosure is highly likely to result in serious and irreparable economic harm despite the technical and organizational measures taken. In such case, Cisco will provide a written justification and notify the competent authority without undue delay.

4. Technical Protection Measures

Cisco applies appropriate technical protection measures to prevent unauthorized access to Requested Data and to ensure compliance with these Data Access Terms and the Agreement, as described in the respective Disclosure Documents. You agree not to alter, remove, or interfere with such technical protection measures.

5. Transfer of Use

If You transfer the Connected Product or Related Service to a new user subject to all applicable Cisco policies, the new user is entitled to access the relevant Requested Data in accordance with the Data Act, subject to appropriate identification and Cisco's standard access verification procedures, per Article 4(5) of the Data Act. Following the transfer, the previous user may no longer access the data unless otherwise permitted under a separate legal basis.

6. Data Access Changes

Cisco may, in good faith, change details regarding the specifications for the data or access arrangements where the change is objectively justified. Objective justifications include, for example, technical modifications of the Cisco Offer or

a change in the Data Holder's infrastructure. Cisco will provide notice of a change to You without undue delay after deciding on, or learning about, the change. Where the change affects Your data access or use in a material way, Cisco will give notice to You at least 30 days before the change takes effect, except where 30 days' notice is impossible or unreasonable under the circumstances, such as addressing the detection of a security vulnerability. Cisco agrees to work with You in good faith to restore any loss of access following such changes.

7. Remedies

If You cannot access the Requested Data or identify another violation of these Data Access Terms, You must give Cisco a detailed description of the alleged violation to allow Cisco to understand and evaluate the alleged violation under Article 37 Data Act. If Cisco fails to cure any alleged violation of the Data Access Terms within 30 days following receipt of Your notice, You have the right to lodge a complaint alleging a violation of the relevant provisions of the Data Act with the competent authority designated by each member state.

8. Third-Party Data Access

8.1 If You wish to grant a third party access to the Requested Data, You must (i) make a request on behalf of the third party, and (ii) ensure the third party understands and complies with (and does not knowingly violate) these Data Access Terms and any Applicable Law. Further, You are solely responsible for (1) any act or omission of an authorized third party granted access and (2) ensuring that any authorized third party granted access only uses the granted access to access or use Requested Data. Cisco reserves the right to suspend or deny access to any third party where the above conditions are not met or in case of suspected misuse or breach of obligations.

8.2 Where Cisco acts solely as a data processor on behalf of a data controller, Cisco is not deemed a Data Holder under Article 2(13) of the Data Act. In accordance with Article 4(10) of the Data Act, access requests concerning Personal Data must be handled by the data controller. Cisco will only facilitate such access upon express instruction from the controller, in line with Articles 28 and 29 GDPR.

9. Definitions

Term	Meaning
Access Method	A Cisco API or other in-product feature made available by Cisco for a Cisco Offer and the associated documentation to enable access to data generated by Connected Products or Related Services pursuant to Regulation (EU) 2023/2854.
Agreement	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).
Cisco API	An application programming interface used as an Access Method.
Connected Product	The definition in Article 2(5) of the Data Act.
Data Access Terms	These Data Access Terms.
Data Act	Regulations (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonized rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act).
Data Holder	The definition in Article 2(13) of the Data Act.
Data Protection Laws	All Applicable Laws that apply to the processing of Personal Data under the Agreement.
Data Subject	A natural person who can be identified, directly or indirectly, as defined in Article 4(1) of the General Data Protection Regulation (Regulation (EU) 2016/679).
Related Service	The definition in Article 2(6) of the Data Act.
Requested Data	Customer Systems Information and Customer Content as listed in the respective Disclosure Document, including a description of the type or nature, estimated volume, collection frequency, storage location, duration of retention of the data.

Exhibit A – API License Terms and Conditions

This Exhibit sets forth the terms and conditions that apply to Your use of the Cisco API.

1. API License Terms and Conditions

By accessing, downloading, copying, distributing, calling, or otherwise making any use of the Cisco API, You accept and agree to be bound by the following terms. All use of the Cisco API must be in accordance with this Exhibit A, and all rights not expressly granted are reserved.

2. Intellectual Property Rights to Cisco API

The Cisco API, in whole or in part, in all forms, is the sole and exclusive intellectual property of Cisco. This Exhibit does not grant You permission to use any trade names, trademarks, service marks, or product names of Cisco. If You provide any feedback or suggestions to Cisco regarding the Cisco API, You grant Cisco (and its Affiliates) a perpetual, irrevocable, worldwide, sublicensable, fully paid-up, royalty-free, and non-exclusive license to use any feedback and suggestions for any purpose without restriction or any obligation of compensation. Subject to Applicable Laws, if You initiate or participate in any litigation against Cisco, its partners, or its customers (including cross-claims and counter-claims) alleging that the Cisco API or its use infringe any patent, copyright, or other intellectual property right, then all rights granted to You under this Exhibit terminate immediately.

3. Cisco's License Grant to You

Subject to the Data Access Terms and this Exhibit, Cisco hereby grants to You (and Your Authorized Users) a perpetual, worldwide, non-exclusive, non-transferable, non-sublicensable, royalty-free license to use and make calls to the Cisco API for the sole purpose of accessing Requested Data as described above. You (and Your Authorized Users) shall not redistribute, resell, or sublicense the Cisco APIs or access to the Cisco APIs.

4. API Termination

You may stop using a Cisco API at any time without notice. Subject to Applicable Laws, Cisco reserves the right to (i) terminate these Data Access Terms and/or this Exhibit, (ii) discontinue the Cisco API (or any portion thereof), (iii) restrict Your (or any of Your Authorized Users') access to or via the Cisco API, or (iv) any combination of (i), (ii), or (iii), for any reason and at any time, without liability or obligation to You.

5. Security

You represent and warrant that any of Your application(s) (or any application(s) of Your authorized third parties) are designed and implemented to operate with a Cisco API in a secure manner. You are responsible for ensuring that Your network, application(s), and the software on Your underlying infrastructure (collectively, "Your Systems") are properly configured, regularly updated, and maintained to securely operate and remain free from known security vulnerabilities. You agree to promptly address any identified vulnerabilities and implement industry-standard security measures, including encryption, access controls, and security monitoring, to protect against unauthorized access or data breaches. You will permit Cisco reasonable access to Your Systems upon request and with adequate prior notice, for the purpose of monitoring compliance with these Data Access Terms and assessing the security of Your Systems.

6. Cisco API Support

Cisco APIs are made available on an "as is" basis. Cisco does not offer direct technical support for these APIs, but we encourage You to explore the available documentation and resources for guidance. Service Level Terms applicable to Cisco Offers do not extend to a Cisco API. Unless otherwise mentioned in the specific Cisco API documentation, backward compatibility is not guaranteed. If a Cisco API is not available, Cisco will provide You access to Requested Data as described in Section 2.2 of these Data Access Terms.