EU Digital Operational Resilience Act Regulatory Terms

GENERAL PROVISIONS

1. Background.

1.1. These EU Digital Operational Resilience Act[1] ("**DORA**") Regulatory Terms (the "**Regulatory Terms**") apply to Supplier in the event Supplier Services are included in or distributed alongside a Cisco Offer that is delivered to Financial Entities regulated by DORA, and are incorporated into the applicable agreement between Cisco and Supplier for the provision of Supplier Services (the "**Agreement**"). Unless stated otherwise herein, in the event of a conflict between the Regulatory Terms and the Agreement, the provisions of the Regulatory Terms will control unless the terms of the Agreement are stricter, in which case the stricter provisions will apply.

1.2. Under DORA, Financial Entities are obliged to impose certain mandatory contractual obligations on Cisco acting as an Information Communication Technologies ("**ICT**") third-party service provider, and indirectly on Cisco's suppliers (i.e., ICT Subcontractors under DORA).

1.3. These Regulatory Terms do not create any rights (express or implied) that Supplier or Supplier's Subcontractors will be entitled to enforce against Cisco or Cisco Customers.

2. Supplier Commitments. During the term of the Agreement, Supplier will:

2.1. Promptly, not later than within forty-eight (48) hours from obtaining relevant information, inform Cisco of any circumstances that may impair the performance of Supplier's obligations under the Agreement.

2.2. As it applies to Supplier Services, ensure that any Supplier personnel and each Subcontractor (including any cloud infrastructure provider) is subject to confidentiality, security and data privacy requirements that are at least as protective as the terms included in the Agreement.

3. Location of data and Services.

3.1. Supplier will identify and notify Cisco of any locations (countries or smaller regions) in which Supplier or any Subcontractor processes Cisco Proprietary Data or from which it provides Supplier Services, and further agrees to assess all risks associated with such processing or providing Supplier Services from such locations.

3.2. Supplier or its Subcontractors may only change the location from which it processes Cisco Proprietary Data or from which it provides Supplier Services upon notifying Cisco at least one-hundred eighty (180) days in advance. Notice shall be given through a method as described to Supplier by Cisco. If Cisco or a Cisco Customer objects to any such proposed change, Cisco will notify Supplier of that objection (each a "**Customer Objection**"). If Supplier or its Subcontractors, nonetheless, choose to implement the proposed change, the parties will work in good faith to address the Customer Objection within thirty (30) days of said Customer Objection, failing which, not withstanding anything in the Agreement to the contrary:

a. Cisco shall be entitled to terminate its use of Supplier Services in relation to the objecting Cisco Customer with effect from the date of Supplier's (or its Subcontractors') implementation of the proposed change; and

b. any minimum notice period which would otherwise apply to such termination will not apply.

B SUPPORTING CRITICAL OR IMPORTANT FUNCTIONS

1. Applicability of Section B.

1.1. The obligations of this Section B of the Regulatory Terms will apply only if Supplier Services are included in or distributed alongside a Cisco Offer provided to Financial Entities and have been identified as supporting such Financial Entities' critical or important functions under DORA.

[1] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011, as amended and replaced from time to time.

2. Critical Subcontractors obligations.

2.1. Supplier will:

a. Require that its Critical Subcontractors contractually agree to obligations at least as strict as those described in these Regulatory Terms; and

b. Oblige its Critical Subcontractors to ensure that contracts with their Critical Subcontractors are at least as strict as these Regulatory Terms, and, further, ensure that those Critical Subcontractors undertake the same efforts further down the subcontracting chain as necessary under DORA.

3. Additional information request.

3.1. Supplier will provide Cisco with up-to-date information allowing the identification of Supplier, its Critical Subcontractors and their ultimate parent undertakings (if any), including:

i. Legal name;

ii. Locations (registered seat);

iii. Corporate registration number (where relevant);

iv. VAT number (where relevant); and

v. Legal Entity Identifer (LEI) (where relevant).

Supplier will notify Cisco of any changes to such information during the term of the Agreement through the method as described by Cisco to Supplier.

3.2. If so reasonably requested by Cisco or a Cisco Customer, Supplier shall provide necessary information proving that Supplier or its Critical Subcontractor has the business reputation, sufficient abilities, expertise and adequate financial, human and technical resources, information security standards, appropriate organizational structure, risk management and internal controls and, if applicable, the required authorization(s) or registration(s) to provide Supplier Services supporting a Cisco Offer delivered to Financial Entities and has been identified as supporting such Financial Entities' critical or important functions under DORA.

4. Audit and Access Right.

4.1. Cisco, Cisco Customer(s) and its Competent Supervision Authority, and any other auditor appointed by Cisco, Cisco Customer(s) or its Competent Supervision Authority, will be granted the right to audit and monitor, on an ongoing basis, the Supplier's performance under the Agreement, as necessary under DORA ("Audit and Access Right"). For the avoidance of doubt, the meaning and scope of the Audit and Access Right described above shall be interpreted in accordance with the provisions of DORA, Regulatory or Implementing Technical Standards issued under DORA, and any applicable regulatory guidelines, as amended or replaced from time to time, including but not limited to Article 30, paragraph 3 of DORA.

4.2. Cisco Customer(s) and the appointed auditor or Competent Supervision Authority will be bound by a statutory or legal confidentiality obligation before executing their Audit and Access Rights.

4.3. Where required, Supplier and its Critical Subcontractors will participate in pooled audits and ICT testing, including threat-led penetration testing, organized by Cisco Customer(s) or Cisco, as the case may be.

4.4. Supplier and its Critical Subcontractors will fully cooperate with Cisco, Cisco Customer(s) and its Competent Supervision Authorities in any regulatory queries, proceedings and other mandatory regulatory activities.

4.5. If an audit reveals that Supplier or its Critical Subcontractor are non-compliant with the Supplier's contractual, regulatory, or legal obligations under the Agreement or applicable laws, Supplier shall take, or will cause that its Critical Subcontractor take, immediate action to correct all non-compliances, and Supplier or its Critical Subcontractor, as the case may be, shall pay for the cost of such corrective efforts. In the event Supplier or its Critical Subcontractor fails to correct all non-compliances within thirty (30) days of written notice, notwithstanding anything in the Agreement

to the contrary, Cisco shall be entitled to terminate its use of the applicable Supplier Service, and any minimum notice period which would otherwise apply to such termination will not apply.

5. Business Continuity and Disaster Recovery

5.1. Supplier will be responsible for establishing, implementing, periodically testing, and maintaining an effective business continuity plan (including disaster recovery and crisis management procedures) to provide continuous access to, and support for, Supplier Services to Cisco and Cisco Customer(s). At all times during the term of the Agreement, that plan will meet or exceed the criteria set forth under the Agreement, or in its absence, the criteria provided in Article 11 of DORA. Supplier will promptly implement the disaster recovery procedures required under the disaster recovery plan upon the occurrence of a disaster (as defined in the plan). In the event Supplier fails to meet its obligations under this Section 5.1 within thirty (30) days of written notice, Cisco shall be entitled to terminate its use of the applicable Supplier Service, and any minimum notice period which would otherwise apply to such termination will not apply.

5.2. Supplier and its Critical Subcontractors will reasonably cooperate with Cisco in supporting Cisco Customers in the orderly transfer of the outsourced functions in the event of the termination of Supplier Services, including making the Cisco Proprietary Data available to Cisco Customers in a readily accessible format.

6. Other obligations

6.1. Supplier guarantees and remains liable for the performance of all subcontracted obligations and agrees to include any applicable provisions of the Agreement in subcontracts with its Critical Subcontractors based on the character of Supplier Services, including the ICT security standards and security features, as well as confidentiality obligations of at least the same standard as provided in the Agreement.

APPENDIX 1

Glossary of Terms

Unless otherwise specified in this Appendix 1 or these Regulatory Terms, capitalized terms used in the Regulatory Terms will have the meanings given them in the Agreement.

1. 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 over 50% of the relevant party; or (b) be able to direct the affairs of the relevant party through voting rights or other lawful means (*e.g.*, a contract that allows control).

"Cisco" means Cisco Systems, Inc. or its applicable Affiliate identified in the Agreement.

"Cisco Customer(s)" means any in-scope Financial Entity under DORA that is using a Supplier Service incorporated into or distributed alongside a Cisco Offer.

"Cisco Offer" means an on-demand service that is accessible via the internet and provides software, platform, infrastructure and network product on an "as-a-service" basis, and incidental technology, resources or support that Cisco licenses or sells to Cisco Customers.

"Cisco Proprietary Data" means: (a) all proprietary and confidential data or other information provided by Cisco or Cisco Customers that is received by Supplier through Supplier Services, (b) all materials in any tangible medium of expression that include the information in such materials, that are provided to Supplier by or on behalf Cisco or Cisco's Customers, (c) any data identified as 'Confidential and/or Proprietary' or that could reasonably be assumed to be confidential and/or proprietary, and (d) any derivatives, improvements or modifications of (a)-(c).

"Competent Supervision Authority" means any EU or EU Member State official supervision or resolution authority having authority over a Cisco Customer.

"Critical Subcontractor" means:

a. Supplier's Subcontractor whose disruption would impair the security or continuity of Cisco Offer (including Supplier Services) being provided to Cisco Customer(s), or
b. Supplier's Subcontractor that has access to and processes Cisco Proprietary Data.

"Financial Entity(ies)" means a financial entity referred to in Article 2 paragraph 2 of DORA.

"Subcontractor" means any entity that is engaged or otherwise utilized, directly or indirectly by Supplier to provide the Supplier Services under an agreement and any downstream entities to which any subcontracted entity further delegates or subcontracts any portion of the Supplier Services.

"Supplier" means the supplier or its Affiliate identified in the Agreement.

"Supplier Service(s)" means any service that Supplier is to provide under the Agreement, including without limitation services provided by Supplier or its Subcontractors to Cisco or Cisco Customer(s).