REGIONAL PROVISIONS

The following country and/or regional provisions (the "**Regional Provisions**") shall apply to you, the Subcontractor, when providing services for Cisco in any of the following countries and/or regions, as applicable, pursuant to the Professional Services Subcontract Agreement (the "**Agreement**") between you and Cisco.

Please note if you are performing services in more than one of the areas you should view all of the relevant Regional Provisions to ensure that you meet all Applicable Laws for those countries/regions.

IN ACCORDANCE WITH THE AGREEMENT BETWEEN CISCO AND SUBCONTRACTOR, SUBCONTRACTOR COVENANTS, REPRESENTS AND WARRANTS THAT IT WILL COMPLY WITH THE FOLLOWING REGIONAL PROVISIONS RELATED TO THOSE COUNTRIES OR REGIONS SPECIFIED BELOW.

ITALY PROVISIONS

If Cisco Systems (Italy) S.r.l. is a party to any SOW, such SOW shall be deemed to incorporate the following terms:

1. Italian Legislative Decree:

Subcontractor represents that it is acquainted with the law regulating the administrative responsibility of legal entities for crimes committed by its legal representatives and, more specifically, with the provisions of Italian legislative decree 8 June 2001 n. 231. Subcontractor further represents that it has reviewed the Subcontractor Ethics Policy and Cisco's Code of Business Conduct, as set forth in the Agreement, and shall fully comply, throughout the duration of the Agreement, with the rules and principles there contemplated.

2. Additional Terms and Conditions for Services provided in Italy:

2.1. With regard to safety at the workplace, the parties, after exchanging and sharing the relevant information, and after examining the respective official documents regarding the risks associated with their business activities, limited to what is relevant for the purposes of the Services, have acknowledged that the performance of the Services under this agreement does not generate the occurrence of any risk of interference.

2.2. For all Services performed within Italy and/or for a Customer in Italy, the following terms shall apply in addition to terms in the PSSA (Agreement):

a. "With respect to the personnel, the Subcontractor shall comply with all rules and obligations as established by the applicable laws, collective and individual agreements including, by way of example, the payment of salaries, social security charges, insurances and withholding taxes on the income received by the employees involved in the performance of the Services. The Subcontractor shall also correctly fulfill any other

obligations or charges with respect to the work relationships with the personnel involved in the performance of the Services, also complying with all applicable provisions in terms of safety and hygiene at work (Legislative Decree no. 81/2008 as subsequently amended), hereby undertaking any and all connected liability.

b. Upon Cisco's request and within 5 days, the Subcontractor shall provide adequate and official documentation attesting the correct payment of salaries, social security charges, insurances, withholding taxes (e.g. evidence of the bank transfers for the payment of salaries, DURC, copy of F24 forms, copy of DM10/2 forms, substitute declarations according to Presidential Decree no. 445/2000 etc.)".

2.3. In addition to all indemnities in the Agreement, for all Services performed within Italy and/or for a Customer in Italy, the following indemnity shall apply:

a. "The Subcontractor shall fully indemnify and hold Cisco harmless, for the entire duration of this Agreement and also after its termination, from any request of payment and/or of indemnification and/or from any fine (including criminal, administrative and civil fines) deriving from any breach of the obligations undertaken by the Subcontractor vis-à-vis its personnel, including, but not limited to, the obligations regarding salary, social security, insurances, taxes, and to fully indemnify and hold Cisco harmless from any detrimental consequences (including, in case of dispute, the payment of legal fees to its lawyers) that may derive to Cisco from the application of: (a) Article 1676 of the Italian Civil Code, (b) Article 29 of the Legislative Decree no. 276/2003, as amended, (c) Article 35 of the Law Decree no. 223/2006, as amended and (d) Legislative Decree no. 81/2008, as amended, as well as any claim or action started by the Subcontractor's personnel in connection with alleged employment or de facto relationships with Cisco. Furthermore, the Subcontractor expressly undertakes to indemnify and hold Cisco harmless, for any cost, claim, reimbursement, sanction or any other payment request current or threatened against Cisco according to Article 26, par. 4, of Legislative Decree no. 81/2008 by Subcontractor's employees for damages occurred and not indemnified by INAIL (Mandatory Insurance for Injuries at Work) or by other equivalent insurance compliant with the applicable law provisions"

b. In the event that DUVRI is neither delivered nor produced, the parties agree as follows: "With regard to safety at the workplace, the Parties have exchanged the information limited to what is relevant for the purposes of the Services, on the basis of the indication received by the End User also with regard to the costs for safety at work"

2.4. All capitalized terms used but not defined herein shall have the meanings ascribed thereto in the Agreement.

2.5. Except as modified by this Section 5, all other terms and conditions of the Agreement remain unchanged.

[End of Italy Provisions]

JAPAN PROVISIONS

To the extent Subcontractor provides services to Cisco Systems G.K., a company organized and existing in Japan having its principal place of business at Midtown Tower, 7-1, Akasaka 9-chome, Minato-ku, Tokyo 107-6227 Japan, or performs Services in Japan, under the Agreement or any SOW, the following Japan Provisions apply:

1. Elimination of Antisocial Forces

1.1 Representation. Subcontractor represents that Subcontractor (in case of a corporation, including its directors, officers, senior management and employees) is not an organized crime group as prescribed under Article 2 of the Act on Prevention of Unjust Acts by Organized Crime Groups (Act No. 77 of 1991), a person who is a member of an organized crime group as prescribed in the same article or a semi organized crime group, or a person for whom five (5) years has not yet passed since said person ceased to be a member of an organized crime group or a semi organized crime group, an associate member of an organized crime group or semi organized crime group, a gang-affiliated group or company, a professional troublemaker at stockholders' meetings, a professional political agitator who supports social movements, or special intelligence violence groups, or a person equivalent to or similar to the above (hereinafter referred to as "Antisocial Forces"), and also assure that Subcontractor does not fall under any of the following items and shall promise the same in the future as well:

a. Have a relationship that is recognized as under the control of management by Antisocial Forces.

b. Have a relationship by which it is found that there is actual involvement of Antisocial Forces in management.

c. Have a relationship by which it is found that there is unfair use of Antisocial Forces for the purpose of acquiring wrongful gain for themselves, their own company, or a third party, or to cause damage to a third party.

d. Have a relationship by which it is found that there is involvement such as providing funds, etc. to Antisocial Forces or providing favours to them.

e. Directors, officers or persons substantially engaging in management have a relationship with Antisocial Forces in a socially reprehensible way.

f. Have any other relationship with Antisocial Forces in any way that Cisco considers inappropriate.

1.2 Assurance. Subcontractor will not directly or through use of any third-party commit or tolerate acts that fall under any of the following items (in case of a corporation, including its directors, officers, senior management and employees):

a. Make violent demands

b. Make unreasonable demands that go beyond the limits of legal liability

c. Use threatening behaviour or violence related to a transaction

d. Commit acts that damage the credit of Cisco or interfere with the business of Cisco through spreading rumours of or using fraudulent means or force.

e. Any act equivalent to any of the acts set forth in the preceding items.

1.3 Re-entrustment.

a. Subcontractor shall not re-entrust business or re-re-entrust (including further subsequent re-entrustment to further downstream entities or individuals) business to any person or persons who are found to be Antisocial Forces or any person who falls under any of the items of 1.1. When Subcontractor re-entrusts business (including cases in which the entrusted party re-entrusts business), Subcontractor shall confirm that said third party (in case of a corporation, including its directors, officers, senior management and employees; the same applies hereafter) is not a member of an Antisocial Forces and said third party does not fall under any of the items of 1.1, and Subcontractor shall have the third party make the same promises prescribed under 1.1 and 1.2.

b. If a violation of the preceding paragraph is found, Cisco may request that Subcontractor immediately cancel the agreement related to re-entrustment or take necessary or appropriate measures.

c. The provisions in Paragraph 1.3 b above shall apply in cases where execution of business entrusted by Cisco is entrusted to a third party such as when executing the entrusted business, the re-re-entrusted party further entrusts the business in whole or in part to a subcontractor (including further subsequent re-entrustment to further downstream entities or individuals).

1.4 Cancellation of Agreement in Case of Involvement of Antisocial Forces.

a. If Cisco deems that Subcontractor (in case of a corporation, including its directors, officers, senior management and employees) is in violation to any of 1.1 or 1.2, Cisco may without advance notice or compensation immediately cancel the Agreement in whole or in part.

b. When Subcontractor violates 1.3 a by means of knowingly or negligently unknowingly re-entrust or allow re-re-entrust (including further subsequent re-entrustment) business to a party who is found to be Antisocial Forces or who falls under any of the item in 1.1, Cisco may without advance notice or compensation immediately cancel the Agreement in whole or in part.

c. When Subcontractor falls under the provisions of 1.1 or 1.2, regardless of whether or not Cisco cancels the Agreement, Subcontractor shall, by the due date instructed by Cisco, pay to Cisco as penalty charges an amount equivalent to 10% of the Agreement amount or such amount could be deducted from any amount payable from Cisco to Subcontractor.

d. The preceding paragraph shall not preclude claims for damages by Cisco against Subcontractor regarding damages that Cisco suffers.

e. Should Subcontractor suffer damages as a result of cancellation based on the provisions in 1.1, 1.2, 1.3 or 1.4, Subcontractor shall not make any claim against Cisco.

2. Subcontractor shall at its own discretion and responsibility, determine, conduct and manage instruction to and supervision of its personnel and staffing, selection of its personnel, work allocation, work assignment, redeployment, replacement, performance evaluation, performance management, education and training with respect to its personnel in order to efficiently and appropriately perform the Services.

a. Subcontractor shall solely and exclusively be responsible for and manage any employment-related matters and disputes of its personnel, including any issues regarding safety and health, overtime, employee classification, work environment, harassment, salary and incentive

payments, workers' accident compensation of any of its personnel in connection with the Services.

b. Subcontractor shall solely and exclusively ensure that its personnel strictly abide by any applicable confidentiality and security rules and policies of Cisco, Subcontractor and/or Subcontractor's personnel in connection with the Services. If so requested by Cisco, Subcontractor shall submit a copy of a pledge or confirmation it secured from its personnel.

c. Subcontractor shall, prior to performing the Services, secure and maintain, pursuant to the Act on the Protection of Personal Information of Japan, and any other applicable laws and regulations, appropriate informed consent from Subcontractor's personnel (i) to provide Cisco and Customers and relevant third parties including those who are located outside of Japan any personal information of its personnel; and (ii) to be maintained, processed or used by such Cisco, Customers and relevant third parties. Subcontractor shall submit a copy of such consent to Cisco if requested by Cisco.

d. Subcontractor understands and shall ensure that, notwithstanding Section 2.2 b of the Agreement, all work-related orders from Customer to Cisco and communications with Customers shall be received, processed, conducted and managed by Cisco.

e. Subcontractor understands and shall ensure that, notwithstanding Section 2.6 of the Agreement, Subcontract's personnel shall not be subject to approval by neither Cisco nor Customer and neither Cisco nor Customer shall request replacement of such personnel.

f. Subcontractor understands and shall ensure that, notwithstanding Section 2.6 of the Agreement, Subcontractor shall, in order to perform the Services appropriately and as a sole employer or party who engages with its personnel, determine, adjust, coordinate and manage its personnel's working hours, working rules and holiday schedules including, without limitation, while working on Customer's or Cisco's premises.

3. Any part or all of the provisions of the Agreement that breach or violate applicable laws, including without limitation, the Labor Standards Act, the Employment Security Act and the Act for Securing the Proper Operation of Worker Dispatching Undertakings and Improved Working Conditions for Dispatched Workers, shall be interpreted or, if needed, amended to the minimum extent so as to comply with such laws.

4. Copyrights. All of its right, title and interest in the Subcontractor Work Product" set forth in Article 5.3 in the Agreement include, without limitation, any rights set forth in Articles 27 and 28 of the Copyright Act of Japan.

[End of Japan Provisions]

USA PROVISIONS

If and to the extent Subcontractor provides Services to Cisco Systems, Inc. or performs Services in the United States of America, under the Agreement or any SOW, the following USA Provisions apply:

Executive Orders:

Federal Contractor Requirements. Where Cisco Systems, Inc. is a party to the SOW, the SOW will be subject to the requirements of 41 CFR 60-1.4 and 29 CFR part 471, Appendix A to Subpart A, which are incorporated into the SOW by reference, as applicable. In addition, such SOW will be subject to the requirements of 41 CFR 60-300.5(a) and 41 CFR 60-741.5(a), which are incorporated into the SOW by reference, as applicable. The latter two regulations prohibit discrimination against qualified individuals on the basis of protected veteran status and disability and require affirmative action to employ and advance in employment protected veterans and qualified individuals with disabilities.

[End of Executive Orders]

Patient Protection and Affordable Care Act (the "ACA"):

ACA Coverage. Subcontractor will offer all personnel that Subcontractor assigns to Cisco on a full- time basis (as defined pursuant to the ACA and Treas. Reg. § 54.4980H-3) (the "**Subcontractor Personnel**") the opportunity to enroll in health coverage for themselves, and their dependents as defined in Treas. Reg. § 54.4980H-1 (a)(12). Such health coverage shall, within the meaning of the ACA and Treas. Reg. § 54.4980H-1 et seq., be "minimum essential coverage" that provides "minimum value" and is "affordable" to the Subcontractor Personnel. Subcontractor will offer such health coverage to applicable Subcontractor Personnel as of the first day the Subcontractor Personnel begins works with Cisco.

Premiums. Subcontractor shall charge Cisco a premium agreed to in writing for each Subcontractor Personnel who elects to enroll in health coverage described above on a monthly basis. Upon Cisco request, Subcontractor shall provide certification of coverage within 30 days of written submission of request.

Indemnification. In addition to any other indemnification provisions set forth in the Agreement, Subcontractor shall indemnify Cisco for any and all penalties (including assessable payments under Internal Revenue Code § 4890H) that are assessed to Cisco on account of Subcontractor's failure to offer such health coverage to any Subcontractor Personnel. Cisco's agreement to pay the additional charge described herein shall not in any way be interpreted or construed as an admission of a common law employment or other employment relationship between Cisco and the Subcontractor Personnel for any other purposes. This section is intended to control all indemnification situations between the parties related to the subject matter herein and no limitations or exclusions of any liabilities, or indemnification provisions or exclusions of any liabilities in any other agreements between the parties shall be applicable to this USA Provisions to relieve Subcontractor of its indemnification obligations hereunder. This section shall survive any expiration or termination of the Agreement.

Submission of Invoices. Subcontractor shall submit invoices as set forth in the Agreement. Subcontractor is responsible to invoice Cisco for each Subcontractor Personnel who elected ACA coverage during the period covered by said invoice. As individual participation in coverage is subject to change, Subcontractor shall reconcile premium amounts invoiced for Subcontractor Personnel electing healthcare on a semi-annual basis and invoice/rebate Cisco

in the month thereafter. Failure to comply with this invoicing requirement shall be deemed as breach of agreement and may result in termination of Services.

[End of ACA]

Contingent Workers & Trade Compliance:

Subcontractor acknowledges that contingent workers supplied to Cisco by Subcontractor may be subject to U.S. deemed export regulations governing access to Cisco, or Customer technologies by non-U.S. persons as defined by the U.S. Export Administration Regulations. Subcontractor shall notify Cisco if Subcontractor elects to supply personnel that have or require a visa or work authorization issued by U.S. Citizenship and Immigration Services to work in the U.S., prior to commencement of the work assignment. Said notification shall be provided by contacting ask-tlc@cisco.com. Subcontractor shall coordinate with Cisco to provide any information and documentation requested by Cisco to verify applicable export license and/or trade sanctions authorization requirements for any non-U.S. Person personnel. If export licenses or trade sanctions authorizations are required, Subcontractor shall provide Cisco with information and documents necessary to seek said licenses or authorizations.

[End of Contingent Workers & Trade Compliance]

Business Associate Agreement

For purposes of this Business Associate Agreement (BAA), the Supplier shall be hereinafter referred to as "**Business Associate**."

1. Background

Subtitle F of the Health Insurance Portability and Accountability Act of 1996, Public Law No. 104-191, as amended by the American Recovery and Reinvestment Act of 2009, Public Law No. 111-005, Part I, Title XIII, Subpart D, Sections 1340113409, (the "**HITECH Act**"), (collectively, "**HIPAA**") provides that Supplier comply with standards to protect the security, confidentiality, and integrity of health information; and

The U. S. Department of Health and Human Services has issued regulations under HIPAA (the "**HIPAA Regulations**"), including the Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 and 164, sub- parts A and E, as amended by the HITECH Act (the "**Privacy Rule**") and the Standards for Security of Electronic Protected Health Information, 45 CFR Parts 160, 162 and 164, as amended by the HITECH Act (the "**Security Rule**") (collectively, the "**Privacy and Security Rules**"); and

Sections 164.502(e) and 164.504(e) of the Privacy and Security Rules set forth standards and requirements for Cisco to enter into written agreements with certain business associates that will have access to Protected Health Information (as defined below); and

Business Associate will provide Services under the Agreement as a subcontractor to Cisco on behalf of a Covered Entity (as defined in the Privacy and Security Rules).

2. Definitions

2.1. "**Breach**" shall have the meaning given to such term in 45 CFR Section 164.402.

2.2. "**Designated Record Set**" shall have the meaning given to such term under the Privacy Rule at 45 CFR Section 164.501.

2.3. "**Electronic Protected Health Information**" or "**Electronic PHI**" shall mean Protected Health Information which is transmitted by Electronic Media (as defined in the Privacy and Security Rules) or maintained in Electronic Media.

2.4. "**Individual**" shall have the meaning given to such term under the Privacy and Security Rules at 45 CFR Section 164.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR Section 164.502(g).

2.5. "**Protected Health Information**" or "**PHI**" shall have the meaning given to such term under the Privacy and Security Rules at 45 CFR Section 164.103, limited to the information created or received by Business Associate from or on behalf of Cisco. "Protected Health Information" includes, without limitation, "Electronic Protected Health Information."

2.6. "**Required by Law**" shall have the meaning given to such term under the Privacy and Security Rules at 45 CFR Section 164.103.

2.7. "**Secretary**" shall mean the Secretary of the U. S. Department of Health and Human Services or his or her designee.

2.8. "**Security Incident**" shall have the meaning given to such term under the Security Rule at 45 CFR Section 164.304.

2.9. "**Service**" or "**Services"** means a service offering from Supplier described in an applicable service or offer description, statement of work, or purchase order listed selected by Cisco.

3. Permitted Uses and Disclosures of PHI. Business Associate shall not use or further disclose PHI other than as permitted or required by this BAA or as otherwise Required by Law. In connection with the foregoing and except as otherwise limited in this BAA, Business Associate may:

3.1. Use or disclose PHI to perform functions, activities, or Services for, or on behalf of, Cisco that are necessary to Perform under the Agreement or applicable SOW, provided that such use or disclosure would not violate the Privacy and Security Rules if performed by Cisco;

3.2. Use PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate; and

3.3. Disclose PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate, provided (i) the disclosure is Required by Law, or (ii) Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and will be used or further disclosed only as Required by Law or for the purpose for which it was disclosed to the person, and that the person agrees to notify Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

4. Responsibilities of Business Associate

4.1. **Appropriate Safeguards.** Business Associate shall use appropriate safeguards to prevent use or disclosure of PHI other than as provided for by the BAA. Business Associate shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of Electronic PHI, as required by the Security Rule. In furtherance of compliance with such requirements, Business Associate shall:

a. maintain an information security program that meets or exceeds the level required by the HIPAA Security Rule;

b. maintain policies and procedures for Business Associate's organization, consistent with the HIPAA Privacy and Security Rules and shall identify an individual within the Business Associate's organization who is responsible for enforcement and oversight of such privacy and security policies and procedures;

c. ensure that any and all employees of Business Associate that handle or access PHI undergo ongoing training regarding the safeguarding of PHI;

d. ensure that any and all third parties that access Covered Entity's confidential data or PHI with whom Business Associate contracts or relies upon for the provision of Services also maintain a framework for compliance with the HIPAA Privacy and Security Rules;

e. implement a contingency plan for responding to emergencies and/or disruptions to business that in any way affect the use, access, disclosure or other handling of Covered Entity's data and PHI;

f. maintain and exercise a plan to respond to internal and external security threats and violations, including an incident response plan;

g. maintain policies and procedures that specifically address how security breaches that are identified will be addressed;

h. maintain technology policies and procedures that provide reasonable safeguards for the protection of PHI on hardware and software utilized by Business Associate;

i. ensure that the electronic transmission of PHI is encrypted meeting at least the minimum standards required by Cisco's data security policies and applicable National Institute of Standards and Technology guidelines.

4.2. **Security Survey.** During the term of this BAA, Business Associate may be asked to complete a security survey and/or attestation document designed to assist Cisco in understanding and documenting Business Associate's security procedures and compliance with the requirements contained herein. Business Associate's failure to complete either of these documents within the reasonable timeframe specified by Cisco shall constitute a material breach of the Agreement.

4.3. **Additional Information.** Business Associate shall provide Cisco with information concerning the aforementioned safeguards and/or other information security practices as they pertain to the protection of Covered Entity's PHI, as Cisco may from time-to-time request. Failure of Business Associate to complete or to respond to Cisco's request for information within the reasonable timeframe specified by Cisco shall constitute a material breach of the Agreement. If Cisco has reasonable concern regarding compliance with the terms of this BAA or the occurrence of a breach, Cisco will be granted access to facilities in order to review policies, procedures and controls relating to the compliance with the terms of this BAA.

4.4. **Reporting of Improper Use or Disclosure.** Business Associate shall promptly report to Cisco any use or disclosure of PHI not provided for by the BAA of which it becomes aware, including breaches of Unsecured Protected Health Information (as defined in the Privacy and Security Rules). In addition, Business Associate shall promptly report to Cisco any Security Incident. If Cisco determines that such use or disclosure may constitute a Breach of Unsecured Protected Health Information, Business Associate agrees to provide Cisco written notification of the Breach that includes the following information within three (3) days: (1) a brief description of the incident, including the date of the Breach and the date of the discovery of the Breach; (2) the identification of each individual whose Unsecured PHI was breached; (3) a description of the types of Unsecured PHI that were involved in the Breach; (4) any steps individuals

should take to protect themselves from potential harm resulting from the Breach; and (5) a brief description of actions that Business Associate is undertaking to investigate the Breach, to mitigate harm to individuals, and to protect against any further breaches.

4.5. **Business Associate's Agents.** Business Associate shall ensure that any agent, including a subcontractor, to whom it provides any PHI received from Cisco agrees to the same restrictions and conditions that apply through this BAA to Business Associate with respect to such PHI.

4.6. **Access to PHI.** At the request of Cisco, and in the time and manner designated by Cisco, Business Associate shall make available PHI in a Designated Record set to Cisco as necessary to meet the requirements under 45 CFR Section 164.524.

4.7. **Amendment of PHI.** At the request of Cisco, and in the time and manner designated by Cisco, Business Associate shall make any amendment(s) to PHI maintained in a Designated Record Set pursuant to 45 CFR Section 164.526.

4.8. **Documentation of Disclosures.** Business Associate agrees to document such disclosures of PHI and information related to such disclosures as would be required for Cisco to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR Section 164.528. At a minimum, such information shall include: (i) the date of disclosure; (ii) the name of the entity or person who received PHI and, if known, the address of the entity or person; (iii) a brief description of the PHI disclosed; and (iv) a brief statement of the purpose of the disclosure that reasonably informs the Individual of the basis for the disclosure, or a copy of the Individual's authorization, or a copy of the written request for disclosure.

4.9. **Accounting of Disclosures.** Business Associate agrees to provide to Cisco, in the reasonable time and manner designated by Cisco, information collected in accordance with Section 3.8 (Documentation of Disclosures) of this BAA, to permit Cisco to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR Section 164.528.

4.10. **Governmental Access to Records.** Business Associate shall make its internal practices, books and records, including policies and procedures and PHI, relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of, Cisco available to the Secretary for purposes of the Secretary determining Cisco's compliance with the Privacy and Security Rules.

5. Responsibilities of Cisco. In addition to any other obligations set forth in this BAA, Cisco shall:

5.1. provide to Business Associate only the minimum PHI necessary to accomplish the Services;

5.2. implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of Electronic PHI, as required by the Security Rule; and

5.3. obtain any consent or authorization that may be required by applicable or federal or state laws and regulations prior to furnishing PHI to Business Associate.

6. Term and Termination. The term of this BAA shall commence as of the Effective Date and continue coterminous with the Agreement unless otherwise terminated as set forth herein. Upon Cisco's knowledge of a material breach by Business Associate of this BAA, Cisco shall either (i) provide an opportunity for Business Associate to cure the breach or end the violation within the time specified by Cisco, or (ii) immediately terminate this BAA if cure is not possible. Upon termination of this BAA for any reason, Business Associate shall return or destroy all PHI received from Cisco, or created or received by Business Associate on behalf of Cisco, and shall retain no copies of PHI. In the event that Business Associate determines that returning or destroying the PHI is infeasible, Business Associate shall provide to Cisco notification of the conditions that make return or destruction infeasible. If Business Associate determines that return or destruction of PHI is infeasible, Business Associate shall extend the protections of this BAA to such PHI and

limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI.

7. **Regulatory References.** A reference in this BAA to a section in the Privacy and Security Rules means the section as in effect or as amended, and for which compliance is required.

8. **No Agency Relationship.** Each Party shall maintain its own independent HIPAA and HITECH Act compliance obligations. The Parties will provide their services as separate legal entities and independent contractors. The Parties expressly agree that no agency relationship is created by this BAA or the underlying Agreement with regard to the individual Parties' HIPAA obligations. Each Party certifies that (1) Cisco shall not have the right or authority to control Business Associate's conduct in the performance of services or in the performance of HIPAA obligations; (2) Cisco shall not have the authority to direct the daily performance of services by Business Associate; and (3) Cisco shall not have the right to give interim instruction to Business Associate regarding the performance of services.

9. **Interpretation.** Any ambiguity in this BAA shall be resolved to permit Cisco to comply with the Privacy and Security Rules.

[End of Business Associate Agreement]

[End of USA Provisions]

UNITED KINGDOM PROVISIONS

To the extent Subcontractor provides services to Cisco International Limited, registered in England and Wales having a principal place of business at 9-11 New Square Park, Bedfont Lakes, Feltham, England TW14 8HA, United Kingdom, and performs Services in the United Kingdom under the Agreement or any SOW or uses a contingent worker who is tax resident in the UK to perform such Services, the following provisions apply:

Cisco IR35 Policy

Supplies of labour

Cisco will not accept or renew engagements for labour where the contingent worker is engaged via a Personal Service Company ("PSC") (whether directly or via a supplier) where Cisco would be considered the end user client under the IR35 off-payroll working rules in United Kingdom which are in Chapter 10, Part 2 of Income Tax (Earnings and Pensions) Act 2003 ("ITEPA") and the Social Security Contributions (Intermediaries) Regulations 2000 as amended from time to time (the "IR35 Rules").

A PSC for these purposes is the contingent worker's intermediary which may be a company (in which the contingent worker and/or their family holds any shares irrespective of the size of their shareholding), a partnership or an individual.

Cisco requires all UK contingent workers providing labour services to be engaged as an individual and to be directly employed by a UK supplier (e.g., a temporary work agency or an agency), with the Subcontractor or supplier as appropriate complying with all its tax obligations as the employer including deducting employment taxes and employee National Insurance contributions and paying employer National Insurance contributions ("NICs"). The Subcontractor (or

the supplier as appropriate) is required to provide a "UK Employment Confirmation Letter" for each contingent worker using a Cisco approved template, provided at the time of the contingent worker onboarding.

Fully outsourced services

Where contingent workers are not onboarded to Cisco (for example, no Cisco User ID is generated, no system or building access is granted etc.), but are working under a managed service contract, the contingent worker may be engaged by the Subcontractor or a supplier either as an individual employee or via a PSC.

If the contingent worker is engaged via a PSC Cisco will not be the end user client as the contingent worker is not providing labour to Cisco. Instead, the Subcontractor will be the end user client and It will therefore be the Subcontractor's responsibility to conduct a Status Determination assessment for the contingent worker and to comply with all their obligations under the IR35 rules, including providing the contingent worker and any entity with which the Subcontractor contracts with a Status Determination Statement notifying the contingent worker whether the contingent worker is inside IR35 (i.e. a disguised employee) or outside the IR35 Rules and the reasons why; providing a disagreement procedure and if the contingent worker is inside IR35 ensuring that the contingent worker is treated for all tax purposes as an employee of the Subcontractor (or the supplier who is the fee payer for the purposes of the IR35 Rules if different) including deducting employment taxes and employee NICs and paying employer NICs.

If the contingent worker is engaged as an individual, the Subcontractor (or supplier if different) must comply with all its tax obligations as the employer including deducting employment taxes and employee NICs and paying employer NICs.

The Subcontractor will implement any required changes in relation to this provision, including with respect to any supplier arrangements, and ensure full and ongoing compliance with these requirements. Please contact Cisco if you have questions.

Indemnity

The Subcontractor shall indemnify Cisco and keep Cisco indemnified for:

- any claim or demand made by HMRC (or any successor body) against Cisco in respect of any income tax (whether under PAYE or otherwise), employee or employer NICs and apprenticeship levy in respect of sums payable by Cisco to the Subcontractor and/or by the Subcontractor to a supplier and/or by the Subcontractor or supplier to the relevant worker in connection with the Agreement or any SOW and against any interest or penalties imposed in connection with any such tax, or contributions or levy; and

- any legal fees or other costs arising in connection with any failure by the Subcontractor to comply with IR35 legislation and/or Cisco in enforcing its rights under this clause.

The Subcontractor agrees that Cisco may, at its option, satisfy such indemnity in whole or in part by way of deduction from any amounts payable to the Subcontractor pursuant to the Agreement or any SOW. If any amount payable by the Subcontractor is not recovered by Cisco by way of such deduction, the Subcontractor shall pay Cisco the outstanding amount within 14 (fourteen) days of receiving a written request from Cisco.

[End of United Kingdom Provisions]

GERMANY PROVISIONS

Additional Terms and Conditions for Services provided in Germany: Non-Integration of Subcontractor Representatives

1.1. Subcontractor's Services provided in accordance with this SOW is not dependent on a specific Subcontractor employee. The participation of a designated Subcontractor employee does not entitle Cisco/Customer and/or the End User to the performance by that specific Subcontractor employee.

1.2. Cisco, Customer/End User and Subcontractor will organize the service delivery and receipt in a way that operational integration of the Subcontractor employee does not occur and no labour-law related instructions are given to the Subcontractor employee by Cisco and/or the Customer/End User.

1.3. Risks with regard to the Subcontractor employees' integration connected or related to the provision of services to Cisco for Customer/End Customer shall be avoided by Subcontractor and the statutory framework regulations, in particular the German Act on Temporary Employment (Arbeitnehmerüberlassungsgesetz, "AÜG") and the jurisdiction on the use of external employees for the provision of services, shall be complied with.

1.4. Cisco and/or the Customer/End User will not treat Subcontractor employees as their own employees, in particular will not integrate them into operational organization and will not give them labour-law related instructions. This shall avoid consequences of ostensible self-employment or a sham contract for services or on the production of work.

1.5. Subcontractor's Project Manager or named representative serves as the single-point-of contact of Cisco and Customer/End User for all directions and instructions of Cisco and/or the Customer/End User to Subcontractor in regards to the performance of the services described in the SOW and has to be given in writing via an e-mail-alias routed to Subcontractor's Project Manager or named representative.

[End of Germany Provisions]

MEXICO PROVISIONS

When subcontractor provides on-site Services at Cisco Systems de Mexico, S. de R.L. de C.V. ("**Cisco Mexico**") or at its Customer(s)'s site or premises in Mexico ("**On-Site Services**"), under this Agreement or any SOW thereof, Subcontractor must, in accordance with Articles 13, 14 and 15 of the Mexican Federal Labor Law ("**FLL**") comply with following requirements:

- Subcontractor will be authorized to render Specialized Services in accordance with the FLL and provide evidence of such authorization to Cisco Mexico by providing a current and valid REPSE certificate.
- Subcontractor must be incorporated in Mexico and be in good standing with its labor and tax obligations.
- Subcontractor's corporate purpose will not be in conflict with Cisco Mexico's own corporate purpose.

Subcontractor shall provide Cisco Mexico with a copy of its corporate by-laws and promptly notify Cisco Mexico of any amendment thereof.

- Subcontractor will not subcontract any portion of the Services rendered in Mexico.
- Subcontractors will provide to its own employees all materials and tools necessary for the provision of the On-Site Service.
- Subcontractor will maintain the registry of its workers before the Mexican Institute of Social Security in the correct risk class, registered under the correct Social Security Regime contributing with real wages and, shall demonstrate and report to Cisco Mexico in the specified period(s) and methods established in FLL for such purposes along with any reasonable information required by Cisco Mexico in accordance with FLL. Such registry and other information will be provided by Subcontractor requested by Cisco Mexico and/or Cisco Mexico's agents for that purpose through the tools and systems established for such purpose.
- Subcontractor will obtain any authorization and/or consent from its own employees entitling Cisco to process and control personal data, as well as to disclose such personal data to Customer(s) for the sole purpose of complying with the FLL.

Cisco will be entitled to terminate the relevant SOW(s), this Agreement or both in accordance with Section 10.5(a) of the Agreement, in case Subcontractor is in breach of any of the obligations set forth in these Mexico Provisions.

Indemnity: Subcontractor will indemnify, defend and hold harmless Cisco Mexico and its Affiliates, officers, directors, employees, successors and assigns (collectively the "Indemnified Parties") from and against all claims, suit and action brought against the Indemnified Parties or tendered to the Indemnified Parties for defense and/or indemnification (collectively "Claims"), and for all resulting damages, losses, cost and liabilities (including reasonable attorney and professional fees) (collectively "Losses") that result or arise from any Claim, which in whole or in part, directly or indirectly: (i) alleges Subcontractor failure to timely comply with any of its obligations toward Subcontractor personnel under the FLL; (ii) alleges Cisco's joint responsibility as co-employer of Subcontractor personnel; (ii) alleges that one or more Subcontractor personnel has caused personal injury or damage to tangible property.

In addition to any other indemnification provisions set forth in the Agreement, Subcontractor shall indemnify Cisco for any and all penalties (including assessable payments under Mexican laws and regulations by any competent authority) that are assessed upon Cisco as a result of Subcontractor's failure to comply with any of its obligations under FLL to any of Subcontractor personnel. Cisco's agreement to pay any of such penalties shall not in any way be interpreted or construed as an admission of a common law employment or other employment relationship between Cisco and the Subcontractor Personnel for any other purposes. This section is intended to control all indemnification situations between the parties related to the subject matter herein and no limitations or exclusions of any liabilities, or indemnification provisions in any other agreements between the parties shall be applicable to this Mexico Provisions to relieve Subcontractor of its indemnification obligations hereunder. This section shall survive any expiration or termination of the Agreement.

[End of Mexico Provisions]

BRAZIL PROVISIONS

If and to the extent Subcontractor provides Services to Cisco in Brazil, under the Agreement or any SOW, the following provisions shall apply:

A former employee from Cisco in Brazil shall not be engaged, by Subcontractor, to provide services to Cisco in Brazil within an 18-month period following the date in which the former employee left Cisco. Consequently, Subcontractor shallnot allocate a Cisco former employee, as a resource or subcontractor employee under the Agreement or any SOW, until at least 19 months or more have passed since the resource left Cisco.

In addition to any other indemnification provisions set forth in the Agreement, Subcontractor will indemnify, defend and hold harmless Cisco and its Affiliates, officers, directors, employees, successors and assigns (collectively the "Indemnified Parties") from and against all claims, suit and action brought against the Indemnified Parties or tendered to the Indemnified Parties for defense and/or indemnification (collectively "Claims"), and for all resulting damages, losses, cost and liabilities (including reasonable attorney and professional fees) (collectively "Losses") that result or arise from any Claim, which in whole or in part, directly or indirectly: (i) alleges Subcontractor failure to timely comply with any of its obligations toward Subcontractor personnel; or (ii) alleges Cisco's responsibility as employer or co-employer of Subcontractor's personnel. Furthermore, Subcontractor shall fully indemnify and hold the Indemnified Parties from any request of payment and/or of indemnification and/or from any fine (including criminal, administrative and civil fines) deriving from any breach of any obligations undertaken by the Subcontractor vis-à-vis its personnel, including, but not limited to, the obligations regarding salary, social security, insurances, and taxes. This section shall survive any expiration or termination of the Agreement or any SOW.

[End of Brazil Provisions]

EUROPEAN UNION DORA REGULATORY TERMS

To the extent Subcontractor's Services or Software are included in or distributed as part of a Customer Engagement with a Customer that is regulated by the Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector, the following terms apply: https://www.cisco.com/c/dam/en_us/about/doing_business/legal/docs/DORA-Regulatory-Terms.pdf

[End of European Union DORA Regulatory Terms]
