Business Associate Agreement

This Business Associate Agreement ("**Agreement**") is made and entered into effective as of the date of last signature by each Party hereto (the "**Effective Date**") by and between San Bernardino County ("**Covered Entity**") and its affiliates and Cisco Systems, Inc., and its affiliates ("**Business Associate**"). This Agreement supersedes and replaces any existing business associate agreement(s) or addendum(s) by and between the parties to this Agreement.

Recitals

WHEREAS, 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 13401-13409, (the "**HITECH Act**"), (collectively, "**HIPAA**") provides that Covered Entity comply with standards to protect the security, confidentiality and integrity of health information; and

WHEREAS, the 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

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

WHEREAS, Business Associate will provide the Cisco branded services referred to as Cisco Advanced Services; Cisco Secure E-Mail Phishing Defense (Formerly Advanced Phishing Protection); Cisco Identity Service Engine; Cisco Secure Cloud Analytics (Formerly StealthWatch Cloud); Cisco Umbrella; Cisco Secure Firewall (Formerly NGFW); Cisco Support Services (Including Cisco SmartNet); ThousandEyes; Webex App; Webex Calling (minus Business Texting); Webex Connect; Webex Contact Center; Webex Meetings (the "Services") to Covered Entity. For clarity, this Agreement applies only to paid subscriptions to Cisco Splunk HIPAA-certified Hosted Services to the extent included in the list of Services. It does not apply to Trials, Evaluations, Beta or Free Licenses of Cisco Splunk Hosted Services, Cisco Splunk on-premise products or on-premise component(s) of a hybrid Cisco Splunk offering, or Cisco Splunk Hosted Services that are not HIPAA-certified.

NOW THEREFORE, in consideration of the mutual promises below, the parties agree as follows:

1. Definitions

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

1.2. "Data Aggregation" shall have the meaning given to such term under the Privacy Rule at 45 CFR Section 164.501.

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

1.4. "**Electronic Protected Health Information**" or "**Electronic PHI**" shall mean Protected Health Information which is transmitted by or maintained in Electronic Media (as defined in the Privacy and Security Rules), and for purposes of this Agreement, shall be limited to the information Business

Associate received from or created, maintained, transmitted or received on behalf of Covered Entity as part of the provision of the Services.

1.5. **"Health Care Operations"** shall have the meaning given to such term under the Privacy Rule at 45 CFR Section 164.501.

1.6. "**Individual**" shall have the meaning given to such term under the Privacy and Security Rules at 45 CFR Section 160.103.

1.7. "**Protected Health Information**" or "**PHI**" shall have the meaning given to such term under the Privacy and Security Rules at 45 CFR Section 160.103, limited to the information maintained, created or received by Business Associate from or on behalf of Covered Entity as part of the provision of the Services. "Protected Health Information" includes, without limitation, "Electronic Protected Health Information".

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

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

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

2. Permitted Uses and Disclosures of PHI

Business Associate agrees not to use or further disclose PHI received or created by Business Associate (or its agents and subcontractors) other than as permitted or required by this Agreement or as otherwise Required by Law. In connection with the foregoing and except as otherwise limited in this Agreement, Business Associate may:

2.1. Use or disclose PHI received or created by Business Associate to perform functions, activities or services for, or on behalf of, Covered Entity, provided that such use or disclosure would not violate the Privacy and Security Rules if done by Covered Entity;

2.2. Use PHI received or created by Business Associate for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate; and

2.3. Disclose PHI received or created by Business Associate 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.

2.4. Provide Data Aggregation services to Covered Entity relating to the Health Care Operation of Covered Entity only to the extent that Covered Entity's use of the Services may be deemed Health Care Operations.

2.5. In providing Cisco Splunk HIPAA-certified Hosted Services, incidentally collect fragments of PHI in metadata generated by use of the Cisco Splunk HIPAA-certified Hosted Services. Business Associate may de-identify any such PHI in accordance with the Privacy Rule at 45 CFR 164.502(d) and use, modify, and disclose such de-identified data as permitted by law.

3. Responsibilities of Business Associate

3.1. Appropriate Safeguards. Business Associate shall use appropriate safeguards to prevent use or disclosure of PHI other than as provided for by this Agreement. Business Associate shall implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of Electronic PHI, in compliance with Subpart C of 45 CFR Part 164.

3.2. Reporting of Improper Use or Disclosure. Business Associate shall report to Covered Entity, as soon as reasonably practicable, any use or disclosure of PHI not provided for by this Agreement of which it becomes aware, including breaches of Unsecured Protected Health Information (as defined in the Privacy and Security Rules). Knowledge of any improper use or disclosure by an agent or subcontractor of Business Associate shall not be imputed to Business Associate unless and until such agent or subcontractor shall have reported such improper use or disclosure to the Business Associate representative responsible for the Covered Entity engagement. With respect to Electronic PHI, Business Associate shall, as soon as reasonably practicable, report to Covered Entity any Security Incident. The parties acknowledge and agree that this Section 3.2 constitutes notice by Business Associate to Covered Entity of the ongoing existence and occurrence of attempted but Unsuccessful Security Incidents (as defined herein) for which no additional notice to Covered Entity shall be required. "**Unsuccessful Security Incidents**" shall include, but not be limited to, pings and other broadcast attacks on Business Associate's firewall, port scans, unsuccessful log-on attempts, denials of service and any combination of the above, so long as no such incident results in unauthorized access, use or disclosure of PHI.

3.3. Business Associate's Agents. Business Associate shall ensure that any agent, including a subcontractor, to whom it provides any PHI received from Covered Entity agrees to the same or more stringent restrictions and conditions that apply to Business Associate in this Agreement with respect to such PHI.

3.4. Access to PHI. To the extent that Business Associate maintains PHI in a Designated Record Set, and to the extent that Business Associate maintains the key or has the ability to decrypt the PHI in a Designated Record Set, Business Associate shall make such information available to the Covered Entity, and in the time and manner reasonably designated by Covered Entity, to Covered Entity in order to meet the requirements under 45 CFR Section 164.524.

3.5. Amendment of PHI. To the extent that Business Associate maintains PHI in a Designated Record Set, and to the extent that Business Associate maintains the key or has the ability to decrypt the PHI in a Designated Record Set, Business Associate shall make any amendment(s) to such information that Covered Entity directs or agrees to pursuant to 45 CFR Section 164.526, at the request of Covered Entity, and in the time and manner reasonably designated by Covered Entity.

3.6. Documentation of Disclosures. Business Associate agrees to document disclosures of PHI and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR Section 164.528.

3.7. Accounting of Disclosures. Business Associate agrees to provide to Covered Entity, in the reasonable time and manner designated by Covered Entity, information collected in accordance with Section 3.6 of this Agreement, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR Section 164.528.

3.8. 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, Covered Entity available to the Secretary for purposes of the Secretary determining Covered Entity's compliance with the Privacy and Security Rules, subject to attorney-client and other applicable legal privileges or protections.

3.9. Minimum Necessary. Business Associate shall make reasonable efforts to Use, Disclose and request the minimum necessary PHI to accomplish the intended purpose of such Use, Disclosure or request.

3.10. Mitigation. Business Associate shall take reasonable measures to mitigate, to the extent practicable, any harmful effect that is know to Business Associate of a Use or Disclosure of PHI by Business associate or its Subcontractors in violation of the requirements of this Agreement.

4. Responsibilities of Covered Entity

In addition to any other obligations set forth in this Agreement, Covered Entity shall:

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

4.2. 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;

4.3. notify Business Associate of any changes in, or revocation of, permission by an Individual to use or disclose PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI;

4.4. notify Business Associate of any restrictions to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 CFR Section 164.522, to the extent that such restrictions may affect Business Associate's use or disclosure of PHI;

4.5. 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;

4.6. as applicable, comply with the terms of any license agreement associated with the Services; and

4.7. not transmit or include PHI in information Covered Entity submits to Business Associate's Technical Assistance Centers (TAC) or professional services personnel, including within the subject or body of a diagnostic file submitted in the course of filing a support ticket or engaging in a support call.

4.8. Covered Entity will not ask Business Associate to Use or Disclose Protected Health Information in any manner that would be impermissible under Subpart E of 45 CFR Part 164 if done by Covered Entity (or Customer's Covered Entity, if applicable). Nothing herein will restrict Business Associate from using Protected Health Information for Data Aggregation or management, administration, and legal responsibilities of Business Associate as permitted by this Agreement.

5. Term and Termination

5.1. Term. This Agreement will commence on the Effective Date and will terminate upon expiration or termination of all contracts, agreements or arrangements governing the Services, unless terminated earlier by written notice by either Party.

5.2. Termination for Cause.

a) Termination for cause by Covered Entity. Upon Covered Entity's knowledge of a material breach by Business Associate of this Agreement, Covered Entity may require Business Associate to cure the breach or end the violation. If Business Associate does not cure the breach or end the violation, or if no cure or end of the violation is possible, Covered Entity, may either (i) immediately terminate this Agreement (and applicable sections of all contracts, agreements or arrangements governing the Services) upon written notice to Covered Entity or (ii) if termination is not feasible, Covered Entity will report the violation to the Secretary.

b) Termination for Cause by Business Associate. Upon Business Associate's knowledge of a pattern of activity or practice of Covered Entity that constitutes a material breach or violation of Covered Entity's obligations under this Agreement, Covered Entity must take reasonable steps to cure the breach or end the violation. If Covered Entity does not cure the breach or end the violation, Business Associate may either (i) immediately terminate this Agreement (and applicable sections of all contracts, agreements or arrangements governing the Services) upon written notice to Covered Entity or (ii) if termination is not feasible, Business Associate will report the violation to the Secretary.

5.3. Effect of Termination.

a. Except as provided in paragraph 5.3.b., of this Section 5.3, upon termination of this Agreement for any reason, Business Associate shall return or destroy all PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity, and shall retain no copies of the PHI.

b. In the event that Business Associate determines that returning or destroying the PHI is infeasible, Business Associate shall provide to Covered Entity 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 Agreement 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.

6. Regulatory References

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

7. Amendment

The parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy and Security Rules and HIPAA.

8. No Agency Relationship

The parties agree that each individual party shall maintain its own independent HIPAA and HITECH Act compliance obligations. The parties will be providing their services as separate legal entities and independent contractors. The parties expressly agree that no agency relationship is created by this Agreement with regard to the individual parties' HIPAA obligations. Each party certifies that (i) Covered Entity shall not have the right or authority to control Business Associate's conduct in the performance of the Services or in the performance of HIPAA obligations; (ii) Covered Entity shall not have the authority to direct the daily performance of the Services by Business Associate; and (iii) Covered Entity shall not have the right to give interim instruction to Business Associate regarding the performance of the Services.

9. Survival

The respective rights and obligations of Business Associate under Section 5.3 of this Agreement shall survive the termination of this Agreement.

10. No Third-Party Beneficiaries

Nothing express or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than Covered Entity, Business Associate and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.

11. Interpretation

Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the Privacy and Security Rules.

12. Counterparts.

This Agreement may be executed in two or more counterparts, each of which may be deemed an original.

13. Waiver of Consequential Damages

In no event shall Business Associate be liable for any; (i) special, incidental, indirect or consequential damages; (ii) loss of any of the following: profits, revenue, business, anticipated savings, use of any product or service, opportunity, goodwill or reputation; or (iii) lost or damaged data.

14. Entire Agreement

This Agreement represents the entire agreement between the parties regarding Protected Health Information and replaces any prior oral or written communications between the parties, except as agreed in writing by the parties. There are no conditions, understandings, agreements, representations, or warranties expressed or implied. This Agreement may only be modified by a written document executed by both parties.

IN WITNESS WHEREOF, the parties hereto have duly executed this Agreement as of the Effective Date.

San Bernardino County	**Cisco Systems, Inc.**
Authorized Signature	**Authorized Signature**
Name Dawn Rowe	**Name** Steve Kite
Title Chair, Board of Supervisors	**Title** Authorized Signatory
Date	**Date**