AMENDMENT NO. 04 TO CONTRACT NO. 41910 RELEASE NO. T-653(5)

THIS AMENDMENT is by and between the State of Minnesota, acting through its commissioner of Administration ("State"), and Cisco Systems Incorporated, 7900 International Drive, Suite 400, Bloomington, MN 55425 ("Contract Vendor").

WHEREAS, the State has a Contract with the Contract Vendor identified as Contract 41910, April 1, 2012, to March 31, 2017 ("Contract"), to provide Telecom: Network Equipment, Maintenance and Support; and

WHEREAS, Minn. Stat. § 16C.03, subd. 5, affords the commissioner of Administration, or delegate pursuant to Minn. Stat. § 16C.03, subd. 16, the authority to amend contracts; and

WHEREAS, the terms of the Contract allow the State to amend the Contract as specified herein, upon the mutual agreement of the Materials Management Division and the Contract Vendor in a fully executed amendment to the Contract.

NOW, THEREFORE, it is agreed by the parties to amend the Contract as follows:

1. Any and all licensing, maintenance, or order-specific agreements, including any pre-installation or other "click-through" agreements that are allowed by, referenced within or incorporated within the Contract whenever the Contract is used for a State procurement, whether directly or through a Cisco agent or reseller, are agreed only to the extent that the terms within any such agreement do not conflict with the Contract or applicable Minnesota laws and only to the extent that the terms do not conflict with the terms of this Addendum. A State employee's decision to choose "accept" or an equivalent option associated with a "click-through" agreement does not constitute the State's concurrence or acceptance of terms, if such terms are in conflict with the Contract or this Addendum.

2. If the State is required to pay Licensor's audit and collection costs, and/or attorney's fees, State/Customer is only required to pay such costs and/or fees up to an aggregate of $5,000, unless a greater amount is ordered to be paid by a court of competent jurisdiction.

3. Any term that requires the State to indemnify the Licensor that is agreed to by "clicking" or " upon installation" or" incorporating by reference" or some other method other than requiring a signature of the State is only agreed by State to the extent permitted by Minnesota law.

4. This Agreement shall not be construed to deprive the State of its sovereign immunity, or of any legal requirements, prohibitions, protections, or exclusions of liability applicable to this Agreement or afforded to the State by Minnesota law.

5. The State does not agree to any term that is in conflict with the Minnesota Data Practices Act, Minnesota Statutes Chapter 13. To the extent Licensor's materials or products meet the definition of Trade Secret as defined by Minn. Stat. § 13.37, subd. 1(b), the State will protect such materials pursuant to the Minnesota Data Practices Act.

6. The parties agree that the Contract will not automatically renew. Renewals shall only occur upon the mutual written agreement of the parties.

7. Section 1.1.4.1 of Contract Number 41910, Price Contract Exhibit A, of Notification of Contract Award is deleted in its entirety.

8. Section 1.1.4.8 (b) of Contract Number 41910, Price Contract Exhibit A, of Notification of Contract Award is deleted in its entirety and revised to read as follows:

   The Agreement and Hardware and Software warranties ("Warranties") are controlled by and construed under the laws of the State of Minnesota, United States of America, notwithstanding any conflicts of law provisions; and the state courts of Minnesota shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties.

9. Supply Chain Security. Notwithstanding anything else in this Section, this Section does not and shall not limit any other rights of the State under this Contract, including, but not limited to, warranties, acceptance, and

return policy, if any.

a. Security Practices and Preventive Controls. The Licensor will use reasonable commercial efforts to ensure that the Licensor and any subcontractors or third parties involved in assembling, manufacturing, packaging, distributing, handling, warehousing, transporting or shipping State goods, including goods intended to be but not yet delivered to the State, meet all applicable security standards and all applicable local, state, federal, and international laws, rules and regulations (hereinafter "supply chain security").

Licensor must maintain certification/accreditation in an official supply chain security program and comply with that program's security standards for all orders sourced from the Contract. Official supply chain security program includes, but is not limited to, one of the following: ISO 28000 or 27036 (as applicable), SAE AS5553 or other SAE standard (as applicable), Customs-Trade Partnership Against Terrorism (C-TPAT), Authorized Economic Operator (AEO), or other program accepted in writing by the State of Minnesota, Office of MN.IT Services ("MN.IT") and the State of Minnesota, Department of Administration's Materials Management Division ("MMD"). To demonstrate certification/accreditation, Licensor must provide to MMD and MN.IT within one month following the effective date of this Contract or amendment adding this Section, whichever is later, a letter verifying its certification/accreditation in an official supply chain security program. Licensor will promptly notify MMD and MN.IT of any change to its certification/accreditation.

Alternatively, if Licensor is not certified/accredited or loses certification/accreditation, Licensor must complete a MN.IT security form to confirm that it complies with supply chain security. The form will require supporting documentation of any responses and must be completed to MN.IT's reasonable satisfaction.

b. Return/Rejection of Goods.
Notwithstanding anything to the contrary, if a breach of supply chain security has occurred or the State in good faith suspects a breach may have occurred, including evidence that packaging or goods were tampered with or damaged, the State may reject delivery of those goods and/or return any of those goods already delivered. Breach of supply chain security includes, but is not limited to, goods received with viruses, malware or similar security deficiencies, cargo theft, tampering, unauthorized access, or other activities that involve suspicious actions or circumstances. Rejection of delivery or return of goods shall be solely the responsibility and at the cost and expense of the Licensor.

At no additional expense to the State, Licensor must provide within a reasonable time frame replacement goods for any goods that were rejected at delivery or returned due to a supply chain security breach. Any reasonable costs and expenses associated with removal or replacement of the goods will be the responsibility of the Licensor.

10. Meraki Products. The provisions attached hereto as Exhibit A (the "Additional Terms Related to Meraki Products") will apply to procurements of Meraki Products by State. For avoidance of doubt, in connection with procurements of Meraki Products, State or applicable State purchasers will also be bound by the terms of the Meraki Supplementary End User License Agreement available at http://www.cisco.com/web/products/seula/meraki-seula.pdf, and attached hereto as Exhibit B (the "Meraki SEULA") to the extent that such terms do not conflict with the terms of the Contract, including this Addendum, or applicable Minnesota laws. "Meraki Products" means Licensor's line of products branded as the Cisco Meraki cloud-networking products, listed at http://meraki.cisco.com. In addition, several of Cisco's software offerings have additional licensing terms or restrictions (Supplemental End User License Agreements, or SEULAs), which change from time to time, and/or are added as Cisco acquires or develops new software. If State wishes to amend the scope of the services to be provided, additional SEULAs may apply. Cisco reserves the right to add new SEULA terms, which shall be applicable only if agreed in writing with the State in the form of an amendment to the Agreement.

This Amendment is effective beginning July 5, 2016 or upon completion of executed document whichever is later, and shall remain in effect through Contract expiration, or until the Contract is canceled, whichever occurs first.

Except as herein amended, the provisions of the original Contract between the parties hereto are expressly reaffirmed and remain in full force and effect.

IN WITNESS WHEREOF, the parties have caused this Amendment to be duly executed intending to be bound thereby.

1. CISCO SYSTEMS INCORPORATED
The Contractor certifies that the appropriate person(s) have executed this Amendment on behalf of the Contractor as required by applicable articles, bylaws, resolutions, or ordinances.

By: _____
Signature

Vivian Liu
Printed Name

Title: Director, Finance

Date: July 25, 2016

APPROVED BY LEGAL

2. MATERIALS MANAGEMENT DIVISION
In accordance with Minn. Stat. § 16C.03, subd. 3.

By: _____

Title: Acquisition Management Specialist

Date: 8/31/16

3. COMMISSIONER OF ADMINISTRATION
Or delegated representative

Original signed

By: _____

Date: AUG 31 2016

By Mary L. Nelson

EXHIBIT A

Additional Terms Related to Meraki Products

1. Security and Data Protection

Licensor is responsible for the security and protection of State data to the extent Licensor stores, transmits, processes or otherwise has access to State data related to Cloud Services provided under this Contract. The terms, conditions, and provisions of this Security and Data Protection section take precedence and will prevail over any other terms, conditions, and provisions of the Contract, if in conflict. Subsection a. of this Security and Data Protection section survives the completion, termination, expiration, or cancellation of the Contract.

Certain Definitions. For the purposes of this Security and Data Protection section, the following terms have the following meanings:

"Cloud Services" means any Meraki Product that meets the definition of "cloud computing" in U.S. Department of Commerce, NIST Special Publication 800-145 (currently available online at: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf) or enables Licensor to store, transmit, process or otherwise access State data.

"State data" means government data, as defined in Minnesota Statutes section 13.02, subdivision 7.

"Not public data" has the meaning in Minnesota Statutes section 13.02, subdivision 8a.

"Security incident" means the unauthorized access, use, disclosure, modification or destruction of State data or interference with system operations in an information system.

"Privacy incident" means violation of the Minnesota Government Data Practices Act (Minnesota Statutes chapter 13) and/or federal privacy requirements in federal laws, rules and regulations. This includes, but is not limited to, improper or unauthorized use or disclosure of not public data, improper or unauthorized access to or alteration of public data, and incidents in which the confidentiality of the data maintained by Licensor has been breached.

a. Data Ownership. As between Licensor and the State, the State solely and exclusively owns and retains all right, title and interest, whether express or implied, in and to any and all State data. Licensor has no and acquires no right, title or interest, whether express or implied, in and to State data.

Licensor will only use State data for the purposes set forth in the Contract and the Meraki SEULA. Licensor will only access State data as necessary for performance of the applicable Contract/Agreement and in accordance with the Meraki SEULA. Licensor will not access State user accounts except in accordance with the Meraki SEULA and to respond to service or technical problems or at the State's specific request.

The Meraki Products enable customers to delete State data in such a way as to render such data inaccessible and unidentifiable to State or any third party.

In the event Licensor receives a request to release any State data, Licensor must promptly notify the State. The State will promptly give Licensor instructions concerning the release of the data to the requesting party before the data is released. Licensor will use commercially reasonable efforts comply with the State's instructions to the extent such instructions do not conflict with applicable law.

b. Security Incidents. If Licensor becomes aware of a Privacy incident or Security incident regarding any State data, Licensor must promptly report the event to the State and the State Chief Information Security Officer. The decision to notify the affected data subjects and the form of such notice following report of a privacy or security incident are the responsibility of the State. Notwithstanding anything to the contrary in this Contract, Licensor will indemnify, hold harmless and defend the State and its officers and employees for any reasonably foreseeable direct damages, costs and expenses incurred by State and related to any privacy or security incident involving any State data, to the extent such costs were the direct result of Licensor's material breach of the terms of this Section 1. Licensor will reasonably mitigate any harmful effects resulting from any privacy or security incident involving any State data.

Notwithstanding the Limitation of Liability set forth in the Contract, Licensor's liability under this Section 1.b shall not exceed one million dollars ($1,000,000). This Section 1.b states Licensor's entire obligation and

State's sole and exclusive remedy for damages and expenses related to a Security Incident.

c. Security Program. Licensor will make commercially reasonable efforts to protect and secure the State data that Licensor stores, transmits, processes or otherwise has access to and related to the Cloud Services provided under this Contract. Licensor will establish and maintain an Information Security Program ("Program") that includes an information security policy applicable to any and all Cloud Services ("Policy"). Licensor's Program and Policy must substantially align with appropriate industry security frameworks and standards such as the Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures ("PCI DSS").

Upon the State's request, Licensor will make a summary or overview of its Policy available to the State on a confidential, need-to-know basis, along with other related information reasonably requested by the State regarding Licensor's security practices and policies. Unless inconsistent with applicable laws, Licensor and the State must treat the Policy and related information on security practices and policies that are specific to the State as confidential information and as not public data pursuant to Minnesota Statutes section 13.37.

d. Data Management. Licensor will not use State data, including production data, for testing or development purposes (in each case, other than to provide technical support to State) unless authorized in writing by the State Chief Information Security Officer or delegate. Licensor will implement and maintain procedures to segregate State data within the application logic of Licensor's systems, unless otherwise explicitly authorized by the State Chief Information Security Officer or delegate.

e. Data Encryption. Licensor must encrypt all State data in transit. All encryption keys must be unique to State data. Licensor will secure and protect all encryption keys to State data. Encryption keys to State data will only be accessed by Licensor as necessary for performance of this Contract.

f. Data Storage. Licensor warrants that any and all State data in possession of Licensor will be stored, processed, and maintained solely on servers designated by Licensor and that no such data at any time will be processed on or transferred to any portable computing device or any portable storage medium, unless that storage medium is in use as part of the Licensor's designated backup and recovery processes.

g. Data Center and Monitoring. During the term of the Contract, Licensor will make available configuration options in the Meraki Dashboard that enable the State to ensure that Licensor's Meraki Products: (1) locate all production and disaster recovery data centers that store, process or transmit State data only in the continental United States, (2) store, process and transmit State data only in the continental United States. It is understood that Licensor is not responsible for how Internet traffic is routed to its intended destination.

h. Security Audits & Remediation. Licensor will audit the security of the systems and processes used to provide any and all Cloud Services, including those of the data centers used by Licensor to provide any and all Cloud Services to the State. This security audit: (1) will be performed at least annually; (2) will be performed according to PCI DSS; (3) will be performed by third party security professionals selected by Licensor in its sole discretion at Licensor's election and expense; (4) will result in the generation of an audit report or certification ("Licensor Audit Report"), which will, to the extent permitted by applicable law, be deemed confidential information and as not public data under the Minnesota Government Data Practices Act (Minnesota Statutes chapter 13); and (5) may be performed for other purposes in addition to satisfying this section.

Upon the State's reasonable, advance written request, Licensor will provide to the State a copy or summary of the Licensor Audit Report.

Licensor will make commercially reasonable efforts to remediate any material control deficiencies identified in the Licensor Audit Report in a commercially reasonable timeframe.

If the State becomes aware of any other Licensor controls that do not substantially meet PCI DSS requirements, the State may request remediation from Licensor. Licensor will consider in good faith the State's reasonable requests to remediate any such control deficiencies.

i. Insurance and Liability. Licensor warrants that during the Term of the Contract, as part of its Professional/Technical, Errors and Omissions liability policy provided under Section 4 of the General Insurance Requirements, it has and will maintain Network Security and Privacy Liability Insurance. .

This policy shall cover claims which may arise from failure of Licensor's security resulting in, but not limited to, computer attacks, unauthorized access, disclosure of confidential or private information, transmission of a computer virus or denial of service.

Licensor is required to carry the following minimum limits:

$2,000,000 – per claim or event

$2,000,000 – annual aggregate

Note that while each claim may be subject to a limitation of $2,000,000 per claim or event, the annual aggregate limit under the Professional/Technical, Errors and Omissions policy (including Network Security and Privacy Liability insurance) remains at $2,000,000. All other terms of the General Insurance Requirements as set forth in the Agreement shall apply to such coverage.

In the Section of the RFP entitled "General Insurance Requirements" the parties agree that the seventh sentence is deleted and replaced with the following: "Should any of the required insurance be cancelled or non-renewed, Contract Vendor shall replace such insurance and provide to the State a certificate of insurance evidencing the replacement insurance, within ten (10) business days after receipt of such cancellation or modification."

j. Subcontractors and Third Parties. Licensor warrants that no State data will be transmitted, exchanged or otherwise provided to other parties except (i) as specifically agreed to in writing by the State Chief Information Security Officer or delegate, and (ii) to third-party vendors of Licensor who are subject to confidentiality obligations in the course of providing the Meraki Products to State.

k. Compliance with Data Privacy and Security Laws and Standards. Licensor shall comply with all applicable State and federal data privacy and data security laws, rules, and regulations in connection with providing the Meraki Products.

EXHIBIT B

MERAKI SUPPLIMENTAL END USER LCENSE AGREEMENT

Meraki LLC
500 Terry Francois Blvd.
San Francisco, CA 94158
T 415.432.1000

Last Updated October 13, 2015

Supplemental End User License Agreement

We're excited that you are considering jumping on the Meraki train or have already done so. Meraki's goal, in a word, is to make everything about your experience GREAT. And that means the legal stuff, too. We aim to keep our legal terms simple, transparent, and to the point. This Supplemental End User License Agreement (this "**Agreement**") supplements and amends the terms of the Cisco Systems, Inc. ("**Cisco Systems**") End User License Agreement available at the following web address: http://www.cisco.com/go/eula (the "**EULA**"). This Agreement forms a binding agreement between you, the end user ("**Customer**"), Cisco Systems, and its affiliates, including Meraki LLC, Cisco System's wholly-owned subsidiary ("**Meraki**" together with Cisco Systems and its affiliates, "**Cisco**"), , and it governs your purchase and use of the Cisco Meraki products. Please read this Agreement carefully. By using our products, you acknowledge that you have read, understood, and agree to be bound by this Agreement and to use our products in compliance with this Agreement. Please keep in mind that your use of the Products after changes to this Agreement are published at http://www.cisco.com/web/products/seula/meraki-seula.pdf will constitute your acceptance of the changes. Any material changes are considered effective upon the earlier of (i) your continued use of the Products once you know about the changes, and (ii) 30 days after they are published. If you do not agree to the terms of this Agreement, please do not use our products.

The terms "Customer," "you," "your," and "yours" refer to you, the end customer and user of the Products, whether obtained directly from Cisco or through one of our authorized resellers. The terms "Cisco," "Meraki" "we," "us," and "our" refer to Cisco.

Okay, with all that in mind, let's dive in. Heads-up: there's a glossary of defined terms at the end.

Article 1 Licenses and Restrictions.

1.1. Paid Licenses. Subject to the terms and conditions of this Agreement, all the paperwork related to your purchasing being in order, and you actually paying for the Products, Meraki grants you non-sublicensable, non-exclusive, non-transferable licenses (i) to use the Firmware on the Hardware (the "Firmware Licenses"), and (ii) to use the Hosted Software via the Internet (the "Hosted Software Licenses"), in each case until the Co-Termination Date or the earlier termination of this Agreement. The Support Services we provide to you are included in the cost of the Hosted Software Licenses. The Firmware License for each item of Hardware you purchase is contingent upon you purchasing and maintaining a valid Hosted Software License, without which the Hardware will not function.

1.2. Third-Party Licenses. If any of the Products include software provided by a third party, the terms under which that software is provided to you may be found at https://meraki.cisco.com/support/#policies:thirdparty. Don't worry, we've made sure you have the right to use any such software as part of the Products at no additional cost to you.

1.3. Restrictions. Let's play nice together. Don't (and don't permit anyone who obtains access to your Network (a "Network User") to) directly or indirectly, reverse engineer the Products or otherwise attempt to discover the source code or algorithms of Meraki software or hardware.

1.4. Customer Responsibilities. Similarly, please use the Hardware only in accordance with the specifications (the "Specifications") available on our website, and keep in mind that you (not Meraki) are solely responsible for maintaining administrative control over your Hosted Software account. And, of course, it is your responsibility to comply with all applicable laws in your use of the Products.

Article 2 Ownership; Customer Data.

2.1. Meraki Rights. As between you and Meraki, Meraki owns and reserves all rights with respect to the Software and all intellectual property rights with respect to the Hardware. In addition, you hereby assign to Meraki all of your interest in any feedback you convey to us related to the Products. Meraki may incorporate modifications into the Hosted Software, the Firmware and the Documentation at any time.

2.2. Customer Data. By using the Hardware, you understand and agree that you are collecting data regarding the devices that connect to your Network and how your network is being used, including the types of data described below. By means of the Hardware, you are then transferring that data to Meraki for processing and storage, including data that may contain personally identifiable information of your Network Users (collectively, "Customer Data"). That said, the Products include functionality that limits or restricts the types of information collected, and you may certainly make use of that functionality. We process and store Customer Data exclusively for the purpose of providing the Products to you, except to the extent necessary to protect our rights in any dispute with you or as required by law. It is your responsibility to provide notice to, and obtain any necessary consents from, your Network Users regarding collection, processing, and storage of Customer Data.

2.2.1. Traffic Information. "Traffic Information" means information about devices that connect to your Network, such as MAC address, device name, device type, operating system, geolocation information, and information transmitted by devices when attempting to access or download data or content (e.g., hostnames, protocols, port numbers, and IP addresses) via the Network. We process and store Traffic Information on your behalf so you can monitor the use and performance of your Network and exercise control (such as network traffic shaping) over the traffic on your Network.

2.2.2. CMX. By enabling and using CMX, you collect the MAC address and relative signal strength of WiFi-enabled devices that are within range of your wireless Network. Meraki does not store these MAC addresses on its servers, except in a de-identified form, and they are not stored on your Hardware. Meraki has no responsibility for whether and how you configure the API to transfer this data to non-Meraki servers or what happens to this data following such a transfer.

2.2.3. Systems Manager. If you choose to use Systems Manager, certain agent software must be installed on the mobile devices, laptops or other devices you choose to enroll. You will then, depending on the type of device, be able to perform remotely actions such as accessing and deleting files, tracking location, enforcing policies, and installing and removing apps.

2.3. Publicity. We won't use each other's name or trademarks without written consent, but we may use your company name and logo in customer lists on our website and collateral.

Article 3 Term and Termination.

3.1. Term. This Agreement will be effective until the expiration of the Term (the "Co-Termination Date"), unless earlier terminated per Section 3.2, below. If you subsequently purchase additional Hosted Software Licenses, the Co-Termination Date will be adjusted so that all of your Hosted Software Licenses (including the new ones) terminate on the same date. This adjusted Co-Termination Date is calculated by (i) determining the aggregate amount of time that your new Hosted Software Licenses extend past your existing Co-Termination Date, and (ii) distributing that amount of time among all your Hosted Software Licenses (including both new and existing ones) pro rata based on the one-year list price for each type of Hosted Software License. Further information is at http://meraki.cisco.com/support#policies:licensing.

3.2. Termination. You may terminate this Agreement for any reason effective upon 30 days prior written notice to Meraki. Meraki may suspend your use of the Products at any time if Meraki reasonably believes that you have breached the terms of Sections 1.3 and 2.2; if such breach remains uncured for 10 days following receipt of notice from Meraki, then Meraki may terminate this Agreement immediately. You may terminate this Agreement for cause if we breach any material obligation of ours under this Agreement and fail to cure such breach within 10 days following

receipt of written notice from you. If you terminate this Agreement for cause, you will receive a refund equal to the value of the remaining time on your Hosted Software Licenses.

3.3. Effect of Termination. Upon any termination of this Agreement, the Hosted Software Licenses and Firmware Licenses will automatically terminate. Sections 2.1 and 4.3 will survive any termination of this Agreement.

Article 4 Warranties; Limitation of Liability.

4.1. Service Level Agreement. Meraki uses its best efforts to keep the Hosted Software up and running 24/7, but no one is perfect. The Service Level Agreement available at https://meraki.cisco.com/trust#sla is your exclusive remedy with respect to any interruptions in the availability of the Hosted Software.

4.2. Hardware Warranties. We represent to you that, during the Warranty Period, the Hardware will be free from material defects in materials and workmanship. Hardware not meeting the warranty above will be, at our option, (a) repaired, (b) replaced, or (c) if you are the original purchaser, we will refund the depreciated amount of the price you paid for such Hardware, calculated on a straight-line, five-year basis. All Hardware repaired or replaced under warranty will be warranted for the remainder of the Warranty Period. For any return permitted under Meraki's then-current return policy (available at http://meraki.cisco.com/support/#policies:return), you will request a Return Materials Authorization ("RMA") number in writing with the reasons for the return request. The warranties in this Section are subject to our Product End of Life Policy, available at https://meraki.cisco.com/support/#policies:eol. "Warranty Period" means the greater of one year or the warranty period set forth in the applicable Specification, commencing, in either case, on the date Hardware is shipped to the original customer. **This Section 4.2 is our sole liability and your sole remedy for any breach of warranty by Meraki.**

4.3. Disclaimer of Warranties. Except as set forth in Sections 4.1 and 4.2, Meraki disclaims all warranties, express, implied, statutory, or otherwise, including any implied warranty of merchantability, fitness for a particular purpose, non-infringement, or title. Meraki assumes no responsibility for any damages to Customer's hardware, software, or other materials.

Article 5 Miscellaneous. This Agreement and the EULA constitute the entire agreement between you and us and supersede all prior agreements and understandings about all this stuff. **Failure to exercise any right under this Agreement will not constitute a waiver.** There are no third-party beneficiaries to this Agreement. This Agreement is governed by the laws of California without reference to conflicts of law rules. For any dispute relating to this Agreement, the Parties consent to personal jurisdiction and the exclusive venue of the courts in Santa Clara County, California. Notwithstanding the foregoing, this Agreement shall not be construed to deprive the State of its sovereign immunity, or of any legal requirements, prohibitions, protections, or exclusions of liability applicable to this Agreement or afforded to the State by Minnesota law. Communications we send to you electronically will be deemed to be in writing. Any notice you provide to us under this Agreement will be in writing and sent by overnight courier or certified mail (receipt requested) to the address above. If any provision of this Agreement is found unenforceable, this Agreement will be construed as if it had not been included. **Meraki may assign this Agreement without the consent of Customer to Cisco Systems, Inc. or its affiliates. If there is a conflict between the terms of this Agreement and the EULA, the terms of this Agreement will apply.**

Article 6 Certain Definitions. The following terms not defined elsewhere in this Agreement have the respective meanings set forth below.

"**CMX**" means the Connected Mobile Experience (CMX) features of the Hosted Software.

"**Documentation**" means any user instructions, manuals, Specifications, or other documentation provided by Meraki at https://meraki.cisco.com/support/#documentation that relate to the Products, including any Modifications.

"**Firmware**" means software embedded in or otherwise running on the Hardware.

"**Hardware**" means Meraki hardware products you have purchased, received in a free trial, promotion, or beta test, or otherwise running on your Network.

"**Hosted Software**" means our proprietary, web-based software platform, including the interface known as the "Dashboard," Systems Manager and any API provided by Meraki.

"**Network**" means your local area network, created in whole or in part by use of the Products.

"**Products**" means the Hardware, the Hosted Software, the Firmware, the Documentation, and the Support Services.

"**Support Services**" means the customer support services described at http://meraki.cisco.com/support.

"**Systems Manager**" means Meraki's web-based mobile device management software.

"**Term**" means the term of the Hosted Software Licenses you have purchased or received in a free trial, as modified each time you purchase additional Hosted Software Licenses so that all your Hosted Software Licenses expires at the same time in accordance with the provisions of Section 3.1.