END-USER LICENSE AGREEMENT

FOR CCG'S CYBER SECURITY APPLIANCE

IMPORTANT – READ CAREFULLY BEFORE INSTALLING, ACTIVATING, OR USING ALL OR ANY PORTION OF THE CYBER SECURITY APPLIANCE:

THIS END-USER LICENSE AGREEMENT ("EULA") IS A LEGAL AGREEMENT BETWEEN YOU (DEFINED BELOW) AND CCG (DEFINED BELOW) THAT GOVERNS THE USE OF THE CYBER SECURITY APPLIANCE (DEFINED BELOW). YOU ARE AGREEING TO BE BOUND BY THIS EULA BY (i) INSTALLING, ACTIVATING, OR USING ALL OR ANY PORTION OF THE CYBER SECURITY APPLIANCE, (ii) CLICKING ON THE "ACCEPT" BUTTON BELOW, OR (iii) CONTINUING TO ACCESS OR USE THE CYBER SECURITY APPLIANCE AFTER BEING NOTIFIED OF A CHANGE IN ANY OF THE TERMS OF THIS EULA WITH WHICH YOU DO NOT AGREE. IF YOU DO NOT AGREE WITH THE TERMS OF THIS EULA, DO NOT INSTALL OR USE THE CYBER SECURITY APPLIANCE.

YOU ARE CONSENTING TO THE TERMS OF THE EULA BY YOUR USE OR CONTINUED USE OF THE CYBER SECURITY APPLIANCE.

YOU WILL NOT BE ENTITLED TO A REFUND OF ANY AMOUNTS PAID OR ONCE YOU PLACE THE ORDER.

An amendment or addendum to this EULA may accompany the Cyber Security Appliance. The most current version of this EULA is available on the CCG website: https://www.phen-ai.com/checkmate

The Software, Security Solutions, and Cyber Security Appliance are protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The Cyber Security Appliance is licensed, not sold.

1. DEFINITIONS.

A. "AdminCore" means the hardware Appliance with CCG's proprietary software components of the Security Solutions that provide the central architecture that receives data from the Sensor(s) and provides the active monitoring function, detection, threat hunting, behavioral analysis, penetration testing, scanning, complete visibility of network monitoring, providing security and threat analysis, providing artificial intelligence functions, threat response, and data storage and

retention for CheckMate, and resides either (i) at the Site for end users who entered into CCG's Cyber Security Appliance On-Premises License, or (ii) for end users who entered into CCG's Cyber Security Cloud-Based License, the AdminCore resides at CCG's authorized facilities.

B. "Agreement" means any separate agreement between You and (i) CCG or (ii) CCG's resellers, distributors, or dealers; such agreements may include without limitation, (a) evaluation, installation, support, purchase orders, or similar agreements, or (b) agreements with a unit or agency of the United States government.

C. "Appliance" means all of CCG's hardware components for the AdminCore and the Sensors.

D. "CCG" means Canfield Consulting Group, LLC, d/b/a Canfield CyberDefense Group, a Maryland limited liability company, 4110 Aspen Hill Road, Suite 300, Rockville, Maryland 20853.

E. "CCG Technology" means the Appliance, Security Solutions, Cyber Security Appliances, and Documentation.

F. "CCG Website" means the URL www.phen-ai.com and www.canfieldcyber.com, which are comprised of various web pages, tools, information, software, content, and features, operated by CCG, and are the intellectual property of CCG.

G. "Cloud-Based License" means the definition under Paragraph 2.C.

H. "Confidential Information" means the trade secrets and proprietary information of CCG and its licensors that is not generally known to the public, whether such information is in tangible or intangible form, and includes IP Rights.

I. "Cyber Security Appliance" means the hardware and software component of the AdminCore and the Sensors that are able to provide the cyber-defense solutions that are selected, which may include (i) detecting network problems and insider threats, (ii) providing threat hunting and behavioral analytic detections, which may include penetration testing, scanning, and complete visibility of the network, (iv) monitoring, (v) zero trust, (vi) providing security and threat analysis, (vii) abilities to alert and take appropriate action, and (viii) providing the artificial intelligence functions for CheckMate and Phen.AI.

i. "Cloud-Based Cyber Security Appliance" means CCG's Cyber Security Appliance where the AdminCore resides on the servers at CCG's authorized facilities and the Sensor(s) reside at the Site and communicate with the AdminCore at CCG's authorized facilities, to provide the selected cyber-defense solutions.

ii. "On-Premises Cyber Security Appliance" means CCG's Cyber Security Appliance where the AdminCore and Sensor(s) reside at the Site, to provide the selected cyber-defense solutions.

iii. "Evaluation Cyber Security Appliance" means CCG's Appliance where the AdminCore and Sensor(s) reside at the Site under an Evaluation License, to provide the selected cyber-defense solutions.

J. "Documentation" means the associated media, printed materials, and "online" or electronic documentation distributed with the Cyber Security Appliance or its components describing the use, installation, operation, and maintenance of the Cyber Security Appliance and their Updates.

K. "Evaluation License" means the definition under Paragraph 2.A.

L. "IP Rights" means the intellectual property rights, including copyrights, patents, patents pending, trademarks, and trade secrets, in and to the Appliance, Cyber Security Appliance, Software, Security Solutions, Documentation, algorithms, databases, and the CCG Websites (including related software, images, photographs, animations, video, audio, music, text, and content) owned by CCG or its licensors.

M. "License Term" means the period of time You are authorized to install and use the Cyber Security Appliance for the appropriate license fee paid and any term renewal period for which the appropriate renewal license fee is paid.

N. "On-Premises License" means the definition under Paragraph 2.B.

O. "Permitted Number of Interfaces" means the number of authorized Internet Protocol Version 4 (IPv4) or Internet Protocol Version 6 (IPv6) addresses, other Internet Protocols ("IPs"), devices, or endpoints, from which the Sensor is permitted to collect

data. A “non-permitted interface” is the unauthorized use of the Sensor to collect data from more than the authorized number of IPv4 or IPv6 addresses, IPs, devices, or endpoints, based on the license fee paid and renewal license fee paid, for the License Term.

P. “Security Solutions” means the different components of the application programming interface of the Software that are installed on the hardware Appliance, or other devices, including without limitation, the Appliance for the AdminCore and the Appliance for the Sensors, that permit You to interact with CheckMate and Phen.AI, and exclude the source code and object code of the Software.

Q. “Sensor” means the components of the Security Solutions that reside on the hardware Appliance provided by CCG, and which collect and provide data to the AdminCore for monitoring, analysis, and action.

R. “Service” means the annual services You have elected to receive from CCG under separate service and support policies Agreements, which includes without limitation, telephone and on-site setup and configuration, telephone and on-site support services, bug fixes, updates, and upgrades, training, and such additional services offered by CCG, subject to CCG’s annual service prices.

S. “Site” means the authorized location or locations where the Cyber Security Appliance is installed or the authorized location or locations specified under any Agreement for the installation and use of the Cyber Security Appliance.

T. "Software" means (i) all of the software code (whether as source code, object code, or application programming interfaces) of the all-in-one cybersecurity suite of software applications and products referred to as "CheckMate" and "Phen.AI," which are comprised of CCG's "Phen.AI," "Cognoscenti," "CanSecure," "NeTERS," "SmartLog Analyzer," and "Agent" software, and each of their underlying programs and subroutines, whether provided together, separately, or in combination, directly on the Appliance or its components, or by electronic download, on physical media, or by any other method of distribution, and (ii) Updates.

U. "TOU" means CCG's Terms of Use, as updated from time to time, and located at https://www.canfieldcyber.com/terms-of-use/.

V. "Update" means any upgrades, updates, patches, additions, deletions, and modifications to the Cyber Security Appliance or Security Solutions.

W. "You" means an individual or any legal entity that is permitted to access and use the Cyber Security Appliance, and on whose behalf, it is used during the License Term.

2. TYPES OF LICENSES. CCG provides the following types of licenses:

A. Evaluation License. Upon your request, and at CCG's sole discretion, CCG may provide You with an Evaluation Cyber Security Appliance under an Evaluation License for You to evaluate the Cyber Security Appliance. The Evaluation Cyber Security Appliance shall be designated for "evaluation purposes," "EVAL," or other similar

designations, under a separate Agreement, and permits the installation and use of the Appliance and CCG Technology at the Site for the Permitted Number of Interfaces during the evaluation period. CCG will not charge a license fee for the Permitted Number of Interfaces under the Evaluation License, provided that You promptly return, the Evaluation Cyber Security Appliance within ten (10) days from the end of the evaluation period, or as otherwise agreed under such evaluation Agreement. THE EVALUATION CYBER SECURITY APPLIANCE IS PROVIDED "AS IS". ACCESS TO AND USE OF ANY OUTPUT FILES CREATED BY SUCH EVALUATION CYBER SECURITY APPLIANCE IS ENTIRELY AT YOUR OWN RISK.

B. On-Premises License. CCG's On-Premises License for CCG's On-Premises Cyber Security Appliance permits the installation and use of the Appliance and CCG Technology at the Site for Permitted Number of Interfaces during the License Term upon payment of the license fee and any renewal license fees.

C. Cloud-Based License. CCG's Cloud-Based License for CCG's Cloud-Based Cyber Security Appliance permits the installation and use of the Sensor(s) at the Site for accessing the AdminCore and CCG Technology that reside at CCG's authorized facilities for the Permitted Number of Interfaces during the License Term upon payment of the license fee and any renewal license fees.

3. ACTIVATION OF LICENSE KEY. Where an Internet connection is available, You are required to activate the Cyber Security Appliance by connecting to the CCG Website or a CCG-

authorized Website through the Internet. Where no Internet connection is available, CCG will activate the license key or provide authorization to activate the license key or renewal license key without the use of the Internet.

4. LICENSE GRANT. Subject to your continuous compliance with all the terms of this EULA and payment of the applicable term license fees:

A. With respect to an On-Premises License, CCG grants You a non-exclusive, non-transferable, non-sublicensable, revocable, limited license to install and use the Cyber Security Appliance and Documentation, during the License Term, for monitoring up to the Permitted Number of Interfaces at the Site for your internal production purposes.

B. With respect to an Evaluation License, CCG grants You a non-exclusive, non-transferable, non-sublicensable, revocable, limited license to install and use the Cyber Security Appliance and Documentation, during the evaluation period, for monitoring up to the Permitted Number of Interfaces at the Site for evaluating the Cyber Security Appliance's ability to meet your internal production needs. Except where otherwise provided under an evaluation Agreement, the evaluation period shall be thirty (30) days.

C. With respect to a Cloud-Based License, CCG grants You a non-exclusive, non-transferable, non-sublicensable, revocable, limited license to install and use the Sensor and Documentation at your Site and access the AdminCore at CCG's authorized facilities, during the License Term, for monitoring up to the Permitted Number of Interfaces at the Site for your internal production purposes.

5. LICENSE RESTRICTIONS.

A. No Copies. You may not, and You agree not to make any copies, including backup copies, of the Cyber Security Appliance, Security Solutions, or Documentation.

B. Third-Party. You may not, and You agree not to (i) rent, lease, loan, or use the Cyber Security Appliance, Security Solutions, or Documentation for timesharing or service bureau purposes, (ii) distribute, sublicense, or otherwise provide the Cyber Security Appliance, Security Solutions, or Documentation for use by the public or third parties, (iii) sell, assign, or transfer your rights in the Cyber Security Appliance, Security Solutions, or Documentation to any third party, or (iv) authorize all or any portion of the Cyber Security Appliance, Security Solutions, or Documentation to be reproduced, copied onto, or distributed to, another user's computer.

C. No Concurrent Use. The Cyber Security Appliance and Security Solutions may not be shared, installed, or used concurrentlyon different computers, unless an additional license fee for such use has been paid.

D. Monitoring. The Cyber Security Appliance may not be used to monitor more than the Permitted Number of Interfaces.

E. No Other Networks. No other server or network use of the Cyber Security Appliance is permitted, including use of the Cyber Security Appliance (i) either directly or

through commands, data, or instructions from or to another computer or network, or (ii) for Internet or web hosting services.

F. Proprietary Notices. You may not, and You agree not to remove or alter any trademark, trade name, copyright, or other proprietary notices, legends, symbols, or labels appearing on or in the Cyber Security Appliance, Security Solutions, or Documentation.

G. Export. The Appliance, Cyber Security Appliance, Security Solutions, and Documentation may only be used in the United States, and any export of the Appliance, Cyber Security Appliance, Security Solutions, or Documentation is strictly prohibited. You agree that the Appliance, Cyber Security Appliance, Security Solutions, or Documentation will not be shipped, transferred, exported, or re-exported, directly or indirectly, into any country or used in any manner prohibited by the United States Export Administration Regulation or any other export laws, restrictions, or regulations (collectively the "Export Laws"). You represent, warrant, and covenant that (i) You are not a citizen, an entity, or otherwise located within, formed under, or subject to, an embargoed nation (including Cuba, Iran, Libya, North Korea, Russia, Sudan, and Syria) and that You are not otherwise prohibited under the Export Laws from receiving the Appliance, Cyber Security Appliance, Security Solutions, or Documentation, and (ii) You will not provide the Appliance, Cyber Security Appliance, Security Solutions, or Documentation to any individual subject to the Export Laws.

H. Limited Use. The Appliance, Cyber Security Appliance, Security Solutions, and Documentation may only be used in connection with cybersecurity monitoring and for no other purpose.

I. No Modification. You may not, and You agree not to modify, reproduce, release, perform, display, adapt, translate, disclose, or create derivative works based upon the Appliance , Cyber Security Appliance, Security Solutions, or Documentation. You may not, and You agree not to, integrate any third-party software into the Cyber Security Appliance or Security Solutions, except as authorized in writing by CCG, and then only with full disclosure of any changes or modifications made or authorized by You to such third-party software.

J. No Reverse Engineering. You may not, and You agree not to reverse engineer, decompile, disassemble or otherwise attempt to discover the source code or underlying ideas or algorithms of the Cyber Security Appliance or Security Solutions, or reduce the Cyber Security Appliance or Security Solutions, to human-readable form.

K. Appliance. With respect to the Appliance, You agree (i) not to install any other software on the Appliance, except as authorized in writing by CCG, and (ii) to run only the CCG provided Security Solutions on the Appliance. You agree that You will not break-down, open, disassemble, modify, remove, or replace any parts of the Cyber Security Appliance, its hard drive, or any other components of the Appliance. You further agree that You will not remove any tamper-indicating seals.

L. Benchmarking. You may not, and You agree not to publish or disclose to any third party the results of any testing or benchmarking without CCG's prior written consent, which CCG may withhold in its sole discretion.

6. TERM AND TERMINATION. Upon payment of the license fee, the License Term of this EULA commences on the date of activation of the license key for the Cyber Security Appliance, or such other date as provided under a separate Agreement, and continues for a one-year period term, except that if You received an Evaluation License for the Cyber Security Appliance, the License Term is thirty (30) days from the date of license activation of the Cyber Security Appliance, or such other period as provided under such evaluation Agreement. The license to use the Cyber Security Appliance will remain in effect until terminated:

A. Termination. Except as may be provided under a separate Agreement, your license to use the Cyber Security Appliance and your License Term will terminate:

i. Evaluation Version. Automatically at the end of the evaluation period for the Cyber Security Appliance.

ii. Non-Renewal. Automatically at the end of the License Term, if You have not renewed your license during the License Term.

iii. Failure to Pay Licensing Fee. If You fail to pay the annual license fee or the then-current annual renewal license fees for the Cyber Security Appliance, prior to the end of the License Term; CCG will provide You with email notice that your license to use the Cyber Security Appliance will terminate in thirty

(30) days. If CCG does not receive payment of the necessary license fees within such thirty (30) day period, CCG has the right to terminate your license to use the Cyber Security Appliance at the end of such thirty (30) day period. In the event that You elect to renew your license after the end of such thirty (30) day period, CCG reserves the right to charge You a twenty percent (20%) reinstatement fee, in addition to its then-current licensing fees and the license activation fee.

iv. Permitted Number of Interfaces. In the event You exceed the Permitted Number of Interfaces, CCG will provide You with email notice ten (10) days prior to terminating your license to use the Cyber Security Appliance. You may cure such breach by paying for any additional license fees to increase the Permitted Number of Interfaces, or discontinuing the use of any interfaces, IPs, devices, or endpoints that exceed the Permitted Number of Interfaces, and notify CCG that You have cured your breach. CCG may terminate your license for cause if You violate this paragraph more than two (2) times during any given License Term; CCG will provide You with a two-day (2-day) notice of termination to your email address.

v. Breach of IP Rights. Immediately, if You breach any of the terms of Section 5 ("License Restrictions") or Section 7 ("Confidentiality and Intellectual Property Rights").

vi. Other Breach. Except as provided in Paragraphs iii, iv, and v, under this Section 6.A, if You breach any of the terms of this EULA or any Agreement, CCG may terminate your license to use the Cyber Security Appliance with thirty (30) days' notice to You, unless You cure such defect within such thirty (30) day period, and You notify CCG in writing within such thirty (30) day period that the breach has been cured, to the satisfaction of CCG.

B. Obligations Upon Termination.

i. Uninstallation. Upon the ending of the License Term under Paragraph 6.A., You must cease all use of the Cyber Security Appliance. You will uninstall and delete any Cyber Security Appliance or copies of the Cyber Security Appliance on your computers, networks, or other devices, and provide written acknowledgment to CCG of its deletion.

ii. For Classified Locations. With respect to On-Premises Licenses for On-Premises Cyber Security Appliances for classified locations, the end user is required to destroy and dispose of the hard drives or any components of CCG's AdminCore and Sensors, and the Documentation.

iii. For Unclassified Locations. With respect to On-Premises Licenses for On-Premises Cyber Security Appliances for unclassified locations, the end user is required to destroy and dispose of the Documentation, the hard drives or any components of CCG's AdminCore and Sensors, or reformat the

hard drives and return them to CCG's authorized facilities, as instructed by CCG.

iv. For Evaluation Licenses at Any Location. With respect to Evaluation Licenses for Evaluation Cyber Security Appliances, at any location:

a. Delete Your Data. Prior to returning the Cyber Security Appliance to CCG, You are obligated to delete all your data from the Appliance using secure erasure procedures. CCG shall not be responsible for your data on the returned Appliance.

b. Return of Cyber Security Appliance. CCG will provide You with a return label for the Cyber Security Appliance and Documentation, and You agree to return the Cyber Security Appliance and Documentation within ten (10) days from the end of the license period.

c. Failure to Return. If You fail to return the Cyber Security Appliance and Documentation within ten (10) days from the end of the license period, You will be obligated to pay CCG the cost of the Appliance. You covenant and agree to pay CCG the cost of the Appliance for your failure to return the Cyber Security Appliance.

v. For Commercial Locations. With respect to licenses for On-Premises Cyber Security Appliances, Cloud-Based Cyber Security Appliances, or Evaluation Cyber

Security Appliances, located at commercial and all other locations:

a. Uninstall, Delete, Return, and Failure to Return. In addition to your obligation to comply with Paragraph 6.B.i., You are obligated to comply with subparagraphs a. through c. of Paragraph 6.B.iv.

b. Lockout Rights. Upon termination, for any reason, CCG will have the right to electronically lock-out the Cyber Security Appliance and any copies of the Security Solutions installed on any device.

7. CONFIDENTIALITY AND INTELLECTUAL PROPERTY RIGHTS. The Appliance, Cyber Security Appliance, Security Solutions, Software, Documentation, and any copies of the Cyber Security Appliance and Documentation are the intellectual property of and are owned by CCG and its licensors.

A. Protection. The structure, organization, and code of the Software and Cyber Security Appliance are the valuable Confidential Information of CCG.

B. License, Not Sale. Your right to use the Cyber Security Appliance and Documentation is a license, not sale, and CCG and its licensors continue to own all right, title, and interest, including all copyright, patents, patents pending, trademarks, and trade secrets, to the Software, Cyber Security Appliance, Appliance, Security Solutions, and Documentation.

C. Website. This EULA does not grant You any rights to use the content provided by or through the CCG Websites, nor does it grant any rights to the CCG Websites, other

than the right to use the CCG Websites according to the terms of the EULA or TOU. All title and intellectual property rights (including copyrights, patents, trademarks, and trade secrets) in and to the CCG Websites (including related software, images, photographs, animations, video, audio, music, text, and content) are owned by CCG, its affiliates, or its licensors. All title and intellectual property rights in and to the information and content that may be accessed through the use of the CCG Websites are the property of the respective content owners and are protected by applicable copyright or other intellectual property laws and treaties.

D. Retention of Rights. CCG and its licensors retain all rights not expressly granted to You.

8. CHANGES TO CYBERSECURITY MONITORING OR ACTIVE RESPONSE.

A. Maintenance. CCG and its suppliers reserve the right, at any time, with or without prior notice to You, to restrict or suspend the functionality of the Cyber Security Appliance to perform maintenance activities and to maintain session control.

B. Service or Features. CCG reserves the right to change any of the features, content, or equipment authorized by CCG for use in connection with the cybersecurity monitoring functions or other functions of the Cyber Security Appliance, at any time, with or without notice to You.

C. Updates. CCG reserves the right to periodically update the Cyber Security Appliance remotely, or by providing compact disks or other acceptable media for On-

Premises Licenses where no Internet connection is available, and to make related changes to the settings and Cyber Security Appliance, or any equipment authorized by CCG for use in connection with the Cyber Security Appliance. You agree and covenant to permit such changes and provide access to your computer and interfaces, the Cyber Security Appliance, and any such equipment authorized by CCG for use in connection with the Cyber Security Appliance, except that with respect to On-Premises Licenses where no Internet connection is available, You and CCG will mutually determine the appropriate procedures for implementing such Updates.

D. Access. You agree to provide CCG electronic access via the Internet to the Cyber Security Appliance to activate the Cyber Security Appliance, provide Updates, and perform maintenance activities; where such access may not be available due to security restrictions, You agree to provide CCG personnel physical access to the Cyber Security Appliance to activate the Cyber Security Appliance, provide necessary Updates, and perform maintenance activities at the then-current rates for Services.

E. Responsibility. Notwithstanding anything to the contrary under this Section 8, it is your responsibility to provide the daily operational management and maintenance to ensure that the Cyber Security Appliance is up-to-date in order to provide effective insider threat monitoring or active response, unless You have entered into a separate Agreement with CCG for such daily operational management and maintenance services.

F. No Access. Notwithstanding anything to the contrary under this Section 8, where CCG does not have access to the Cyber Security Appliance for On-Premises Licenses, You covenant and agree that upon receipt of the Updates from CCG, You will install the Updates in your testing environment, test the Updates in your testing environment, and deploy the Updates for production use only after completion of successful testing in your testing environment, unless You have entered into a separate Agreement with CCG to provide such on-premises services.

9. UPDATES.

A. Valid License. If CCG provides Updates to a previous version of the Cyber Security Appliance, You must possess a paid valid current license to such previous version in order to use such Updates. All Updates are provided to You on a license exchange basis. You agree that by using an Update, You voluntarily terminate your right to use any previous version of the Cyber Security Appliance. As an exception, You may continue to use a previous version of the Cyber Security Appliance after receiving the Update but only to assist in the transition to the Update, provided that: (a) the Update and the previous versions are installed on the same Appliance; (b) the previous versions or copies thereof are not transferred to another computer; and (c) You acknowledge that any obligation CCG may have to support the previous versions of the Cyber Security Appliance may be ended upon availability of the Update.

B. Deployment. CCG, from time to time during the License Term and without your separate permission or consent, may deploy Updates of, or replacements for, any Cyber Security Appliance, and as a result of the deployment You may not be able to use the applicable Cyber Security Appliance (or certain functions of the Cyber Security Appliance) until the Update is fully installed or activated. Updates may include both additions to, and removals of, any particular features or functionality offered by the Cyber Security Appliance or may replace it entirely, and CCG will determine the content, features, and functionality of the Updates in its sole discretion. CCG is not required to offer You the option to decline or delay Updates, but in any event, You may need to download and permit installation of all available Updates to obtain maximum benefit from the Cyber Security Appliance. CCG may stop providing support for the Cyber Security Appliance until You have accepted and installed all Updates. CCG in its sole discretion will determine when and if Updates are appropriate and has no obligation to make any Updates available to You.

10. NOTICE TO U.S. GOVERNMENT END-USERS. The CCG Technology is deemed to be "Commercial Products," "Commercial Computer Software," or "Computer Software Documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. Consistent with such regulations, as applicable, the CCG Technology is subject to the terms and conditions herein. All U.S. Government end users acquire the CCG Technology with only those rights set forth in this EULA. Unpublished-rights reserved under

the copyright laws of the United States. Canfield Consulting Group, LLC, 4110 Aspen Hill Road, Suite 300, Rockville, Maryland 20853.

11. COMPLIANCE WITH LICENSES.

A. Certification. You agree that upon request from CCG or CCG's authorized representative, You will within thirty (30) days fully document and certify that the use of any and all Cyber Security Appliances and the Permitted Number of Interfaces, at the time of the request is in conformity with your valid paid licenses from CCG.

B. Records. You grant to CCG and its independent accountants the right to examine your books, records and accounts during your normal business hours to verify compliance with this EULA and any Agreements. In the event such audit discloses non-compliance with this EULA or any Agreement, You shall promptly pay to CCG the appropriate license fees, plus the reasonable cost of conducting the audit.

12. LEGAL AUTHORITY. You represent and warrant that You have the legal authority to enter into this EULA, that You are duly authorized and empowered to execute, deliver, and perform the terms under this EULA and any Agreement, and that such action does not conflict with or violate any provision of law, regulation, policy, contract, or other instrument to which You are a party or by which You are bound, and that this EULA and any Agreement constitutes a valid and binding obligation enforceable in accordance with its terms.

13. MONITORING. You acknowledge that You are responsible for all use of the Cyber Security Appliance and for monitoring the data provided by the Cyber Security Appliance, unless

under a separate Agreement, You have authorized CCG to monitor and manage the data provided by the Cyber Security Appliance.

14. LIMITED WARRANTY, DISCLAIMERS, AND EXCLUSIONS.

A. Limited Warranty. CCG warrants that when properly installed and used in accordance with the Documentation, the CCG Technology will perform substantially in accordance with the Documentation for a period of thirty (30) days from the delivery date of the Cyber Security Appliance. If the CCG Technology does not perform substantially in accordance with the Documentation, your sole and exclusive remedy will be limited to replacement of the Cyber Security Appliance, and where applicable, the Appliance. This limited warranty does not apply if the Appliance, Cyber Security Appliance, Security Solutions, (i) has been altered, except by CCG or its authorized representative, (ii) has not been installed, operated, repaired, or maintained in accordance with instructions supplied by CCG, (iii) has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident; or (iv) is licensed, for beta, evaluation, testing, or demonstration purposes for which CCG does not charge a purchase price or license fee.

B. AS IS. CCG DOES NOT WARRANT THE PERFORMANCE OR RESULTS YOU MAY OBTAIN BY USING THE CCG TECHNOLOGY. EXCEPT FOR THE FOREGOING LIMITED WARRANTY UNDER PARAGRAPH A OF THIS SECTION 14, THE CCG TECHNOLOGY IS PROVIDED ON AN “AS IS” AND “AS AVAILABLE” BASIS AND CCG MAKES NO EXPRESS OR

IMPLIED WARRANTIES, AND TO THE MAXIMUM EXTENT PERMITTED BY LAW, DISCLAIMS ANY AND ALL WARRANTIES IMPLIED BY STATUTE, COMMON LAW, JURISPRUDENCE, COURSE OF DEALING, COURSE OF TRADE, OR OTHER THEORIES OF LAW, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY, SUITABLE QUALITY, FITNESS FOR ANY PARTICULAR PURPOSE, NONINFRINGEMENT OR NONINTERFERENCE OF THIRD PARTY RIGHTS OR TITLE, WITH REGARD TO THE CCG TECHNOLOGY.

C. NO PROVISIONING. WHILE CCG WILL ENDEAVOR TO DELIVER THE CCG TECHNOLOGY ACCORDING TO AN AGREED UPON SCHEDULE, CCG DOES NOT WARRANT THAT THE CCG TECHNOLOGY CAN BE PROVISIONED TO YOUR LOCATION, OR THAT PROVISIONING WILL OCCUR ACCORDING TO A SPECIFIED SCHEDULE, EVEN IF CCG HAS ACCEPTED YOUR ORDER FOR THE CCG TECHNOLOGY.

D. INTERRUPTION. CCG DOES NOT WARRANT THAT THE CCG TECHNOLOGY WILL BE UNINTERRUPTED OR ERROR FREE, THAT THE CCG TECHNOLOGY WILL WORK PROPERLY ON ANY GIVEN DEVICE OR WITH ANY PARTICULAR CONFIGURATION OF THE CCG TECHNOLOGY, OR THAT THE CCG TECHNOLOGY WILL BE COMPATIBLE WITH OR INTEGRATE WITH YOUR COMPUTER SYSTEMS.

E. VIRUSES. CCG DOES NOT WARRANT THAT ANY OF THE CCG TECHNOLOGY, OR OTHER EQUIPMENT AUTHORIZED BY CCG FOR USE IN CONNECTION WITH CYBERSECURITY MONITORING WILL PERFORM AT A PARTICULAR SPEED, BANDWIDTH OR DATA THROUGHPUT RATE, OR WILL BE SECURE, OR FREE OF VIRUSES, WORMS,

DISABLING CODE OR CONDITIONS, OR THE LIKE. CCG SHALL NOT BE LIABLE FOR LOSS OF YOUR DATA, OR IF CHANGES IN OPERATION, PROCEDURES, OR SERVICES REQUIRE MODIFICATION OR ALTERATION OF YOUR EQUIPMENT (INCLUDING ANY OTHER EQUIPMENT AUTHORIZED BY CCG FOR USE IN CONNECTION WITH THE CYBERSECURITY MONITORING), RENDER THE SAME OBSOLETE OR OTHERWISE AFFECT ITS PERFORMANCE.

15. LIMITATION OF LIABILITY. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL CCG OR ITS OFFICERS, DIRECTORS, EMPLOYEES, OR AGENTS (INDIVIDUALLY, IN COMBINATION, OR COLLECTIVELY, THE "CCG PARTIES") BE LIABLE FOR (i) ANY DIRECT, INDIRECT, PUNITIVE, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES WHATSOEVER, INCLUDING DAMAGES FOR LOST PROFITS, LOSS OF REVENUE, BUSINESS INTERRUPTION, LOSS OF INFORMATION, LOSS OF PROGRAMS OR DATA, DAMAGE TO DATA, OR ANY OTHER PECUNIARY LOSS, ARISING OUT OF THE USE, PARTIAL USE, OR INABILITY TO USE THE CCG TECHNOLOGY, OR RELIANCE ON OR PERFORMANCE OF THE CCG TECHNOLOGY, OR THE PROVISION OF OR FAILURE TO PROVIDE SERVICES, REGARDLESS OF THE TYPE OF CLAIM OR THE NATURE OF THE CAUSE OF ACTION, INCLUDING THOSE ARISING UNDER CONTRACT, TORT, NEGLIGENCE, OR STRICT LIABILITY, EVEN IF A CCG PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH CLAIM OR DAMAGES. CCG'S ENTIRE LIABILITY (EXCEPT IN THE CASE OF WARRANTY DEFECTS, IN WHICH CASE YOUR SOLE AND EXCLUSIVE REMEDY IS SET FORTH IN SECTION 14) TO YOU SHALL BE LIMITED TO A MAXIMUM OF UP TO THREE (3) MONTHS OF

YOUR CYBER SECURITY APPLIANCE LICENSE FEE (BUT EXCLUDING ALL OTHER FEES, INCLUDING, HARDWARE FEES, NONRECURRING CHARGES, REGULATORY FEES, SURCHARGES, SERVICE FEES AND TAXES), FOR YOUR THEN-CURRENT VALID LICENSE PERIOD, AND RETURN, AT YOUR EXPENSE, THE APPLIANCE, AND UNINSTALL ALL COPIES OF THE CCG TECHNOLOGY. NO REFUND WILL BE DUE WHERE YOU HAVE NOT PAID A LICENSING FEE.

16. THIRD-PARTY BENEFICIARIES. ALL LIMITATIONS AND DISCLAIMERS STATED UNDER SECTIONS 14 AND 15 ALSO APPLY TO CCG'S THIRD-PARTY LICENSORS, SUPPLIERS, RESELLERS, DEALERS, AND DISTRIBUTORS, AS THIRD-PARTY BENEFICIARIES OF THIS EULA.

17. CLASS ACTION WAIVER. TO THE EXTENT PERMITTED BY APPLICABLE LAW, ANY DISPUTE OR CONTROVERSY BETWEEN YOU AND CCG WILL PROCEED ON AN INDIVIDUAL BASIS AND WILL NOT PROCEED AS PART OF A CLASS ACTION, COLLECTIVE ACTION, PRIVATE ATTORNEY GENERAL ACTION, OR OTHER REPRESENTATIVE ACTION AND YOU AND CCG KNOWINGLY, VOLUNTARILY, INTENTIONALLY AND IRREVOCABLY WAIVE ANY RIGHT TO PROCEED IN A CLASS ACTION, COLLECTIVE ACTION, PRIVATE ATTORNEY GENERAL ACTION, OR OTHER REPRESENTATIVE ACTION OR TO SERVE AS A CLASS REPRESENTATIVE.

18. CONSUMER RIGHTS. THE REMEDIES SET FORTH IN THIS EULA ARE YOUR SOLE AND EXCLUSIVE REMEDIES. YOU MAY HAVE ADDITIONAL RIGHTS UNDER CERTAIN LAWS (SUCH AS CONSUMER LAWS), WHICH DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, OR THE EXCLUSION OR LIMITATION OF CERTAIN DAMAGES. IF THESE LAWS APPLY, CCG’S EXCLUSIONS OR LIMITATIONS MAY NOT APPLY TO YOU.

19. INDEMNIFICATION. You agree to indemnify and hold harmless, and, at CCG's option, defend CCG Parties from and against any and all losses, damages, liabilities, costs, and expenses, including court costs and reasonable attorneys' and experts' fees, related to or arising from any claim, suit, action, or proceeding based on your use of the CCG Technology, or any other equipment used in connection with the cybersecurity monitoring (or the use of the CCG Technology, or any other equipment by anyone else) due to (i) gross negligence or willful misconduct, (ii) use of the CCG Technology in a manner not authorized or contemplated by this EULA and/or the Documentation, (iii) use of the CCG Technology in combination with data, software, hardware, equipment, or technology, not provided by CCG or authorized by CCG in writing, (iv) modification to the CCG Technology not made by CCG, (v) use of any version other than the most current version of the CCG Technology delivered to You, (vi) violation of applicable laws, regulations, any Agreement or this EULA; or (vii) your use in any manner that harms any person or results in the personal injury or death of any person or in damage to or loss of any tangible or intangible (including data) property.

20. THIRD-PARTY SOFTWARE & OPEN-SOURCE SOFTWARE.

A. Prohibition. Except for those third-party software made available for a fee by CCG, CCG does not provide You with third-party software or licenses. You may not install any third-party software on the Appliance or integrate such third-party software into the Security Solutions without CCG's prior written consent, which CCG may withhold in its sole discretion.

B. Election. Certain third-party software may be recommended by CCG for use with the Cyber Security Appliance. Unless CCG has agreed in writing under a separate Agreement to obtain such third-party software and license on your behalf for a fee, it is your responsibility to obtain the third-party software and license at your expense. It is your responsibility to confirm with CCG that such third-party software (and the version of the software) is compatible with the Cyber Security Appliance, and You acknowledge that any installation or integration of such third-party software is undertaken at your sole risk. If agreed in writing under a separate Agreement, CCG may obtain such third-party software and license on your behalf and provide installation services of such third-party software; provided however, it shall be your responsibility to obtain any support services from such third-party software provider under their terms and conditions for the fees prescribed by such third-party software provider, unless under a separate Agreement CCG has agreed to obtain such third-party support and services for the fees prescribed by such third-party software provider.

C. Third-Party Offers. Certain third parties, who provide the servers and components of the Appliance, may offer You the opportunity to acquire software, services, and other products supplied by them or their third parties. Except as otherwise provided under paragraph 20.B, You may not install such third-party software or products on the Appliance or integrate such software or products into the Security Solutions without CCG's prior written consent, which CCG may withhold in its sole discretion.

D. Open-Source. Open-source software not owned by CCG is subject to separate license terms. CCG's use of open-source object code in its Appliance will not (i) materially or adversely affect your ability to exercise your right in the Appliance; or (ii) cause your software to become subject to an open-source license, provided You only use the CCG Technology in accordance with the Documentation, in object code form, and within the permitted scope of CCG's license. CCG makes no representations or warranties, and accepts no liability with respect to such open-source software, if You do not use the CCG Technology in accordance with the Documentation, in object code form, and within the permitted scope of CCG's license.

E. Responsibility. You acknowledge that with respect to all third-party software, including without limitation the open-source software not owned by CCG, the applicable third-party is solely responsible for its offerings and CCG makes no representations or warranties concerning those offerings and accepts no liability with respect to them, and if You acquire or use any such third-party software or offerings, including without limitation the open-source software not owned by CCG, the software and offerings and your use of them will be governed by the applicable license agreements, terms of use, privacy policies, and other terms and conditions required by such third-party. Further, such third-party software may contain links to third-party websites that are not under the control of CCG and CCG is not responsible for, and makes no endorsement of, the

content on such third-party websites, weblinks on such third-party websites, or any changes or updates to such third-party websites.

F. Information. By using any product, service, or functionality originating from a third-party software provider, You acknowledge and consent that CCG may share such information and data with such third-party with whom CCG has a contractual relationship to provide the requested product, service, or functionality.

G. Disable. In the event that authorized third-party software disrupts the Cyber Security Appliance, CCG shall have the right to temporarily disable such third-party software until the problem can be resolved. In the event You install third-party software without CCG's prior written consent, CCG shall have the right to terminate your license for breach under Paragraph 6.A.v.

21. GOVERNING LAW. This EULA will be governed by and construed in accordance with the laws of the state of Maryland without regard to its conflict of laws principles and without regard to the Uniform Computer Information Transactions Act, except that (i) if You are a U.S. Government entity, this EULA is governed by the laws of the United States, and (ii) if You are a state or local government entity in the United States, this EULA and any Agreement is governed by the laws of that state. Any action to enforce this EULA and any Agreement must be brought, exclusively in the State of Maryland and within one year of the date of your discovery of such action. This EULA will not be governed by the United Nations Convention on Contracts for the International Sale of Goods, ("UCITA") the application of which is expressly excluded.

22. INJUNCTION. You agree that any unauthorized use or disclosure of Confidential Information, and/or infringing use of the CCG Technology or any threat thereof, would likely cause CCG or its licensors irreparable harm that could not be fully remedied by monetary damages. Thus, You agree that CCG or its licensors will have the right, in addition to any other remedy available to it, to injunctive or other equitable relief from a court of competent jurisdiction, without proof of actual damages, and without payment of any bond, as may be necessary to prevent any unauthorized use or disclosure of the CCG Confidential Information and/or infringing use of the CCG Technology.

23. EULA. CCG reserves the right to periodically update, change, or revise its EULA. In addition, Updates may be licensed to You by CCG with additional or different terms. This EULA and any Agreement is the entire agreement between CCG and You relating to the Cyber Security Appliance and Documentation, and supersedes any prior representations, discussions, undertakings, communications, or advertising relating to the Cyber Security Appliance. If You have been provided a later version of this EULA with any Agreement, then that version of the EULA will control with respect to any conflict between the EULAs. The latest version of the EULA is posted on the CCG Website, which shall control in the event of a dispute.

24. SEVERANCE. If any part of this EULA is found void or unenforceable, it will not affect the validity of the balance of this EULA, which shall remain valid and enforceable according to its terms.

25. HEADINGS. The headings in this EULA are for convenience and will not be used to interpret this EULA or any Agreement.

26. GENDER AND NUMBER. Except where otherwise indicated by context, any masculine term used in this EULA also includes the feminine, the plural includes the singular, and the singular includes the plural.

27. NOTICES. All notices required to be sent shall be sent to the addresses, facsimile numbers, or email addresses provided to CCG when You activated the Cyber Security Appliance under this EULA or as provided under any Agreement, and shall be deemed given (i) on the date of mailing, if sent by certified mail or by a nationally recognized overnight courier (e.g. Federal Express, UPS, etc.), or (ii) on the date sent, if sent by facsimile transmission or email, provided confirmation of receipt is received. In the event notice is sent under clause (i), postage or delivery costs shall be prepaid. The addresses, facsimile numbers, or email addresses may be changed by each of the parties from time to time by providing notice to the then current address, facsimile number, or email address of the party to receive notice.

28. WAIVER. No failure, delay or omission by a party in exercising any right, power or remedy provided by law or equity under this EULA shall operate as a waiver of that right, power or remedy, nor shall it preclude or restrict any future exercise of that or any other right, power or remedy. No single or partial exercise of any right, power or remedy provided by law or equity under this EULA shall prevent any future exercise of it or the exercise of any other right, power or remedy. A waiver of any term, provision, condition or breach of this EULA shall only be

effective if given in writing and signed by the waiving party, and then only in the instance and for the purpose for which it is given.

29. DURATION. Any terms of this EULA which by their nature extend beyond expiration or termination of this EULA shall remain in effect until fulfilled and shall bind the parties and their legal representatives, successors, heirs and assigns.

30. DISPUTES. In the event of a dispute between the parties, the parties agree to mediate their dispute with a neutral mediator prior to proceeding with any legal action.

By clicking "Accept," You acknowledge and represent that (i) You have read and accept the terms and conditions of the End-User License Agreement on behalf of your organization, and (ii) You are authorized on behalf of your organization to bind your organization to the terms and conditions of this EULA.

[ACCEPT] [DECLINE]