**Cyber Security Appliance and Services Agreement**

Customer agrees to these general provisions for purchase orders placed with Canfield Consulting Group, Inc., d/b/a Canfield CyberDefense Group (“CCG”) for on-premises or cloud-based Cyber Security Appliances:

1. ACCEPTANCE OF CONTRACT/TERMS AND CONDITIONS:
	1. Integration. This Agreement integrates, merges, and supersedes any prior offers, negotiations, and agreements concerning the subject matter hereof and constitutes the entire agreement between the parties.
	2. Acceptance of this Agreement. Customer’s acknowledgement, acceptance of quote, acceptance of purchase order, or payment for the Cyber Security Appliance or Services, shall constitute unqualified acceptance of this Agreement.
	3. Updates. Customer is required to check CCG's website periodically for any updates to this Agreement and the Related Documents at <https://docs.cancgroup.com/partner-nw/agreements>, which shall be effective upon posting. Customer's continued use of the Cyber Security Appliance, Software, or Services after any such update constitutes acceptance of the updated documents. If Customer does not agree to any updated terms, Customer must immediately cease using the Cyber Security Appliance, Software, and Services. Customer acknowledges that by submitting a purchase order, it has reviewed and agreed to all terms contained in this Agreement and the Related Documents.
	4. Other Terms. Any modifications to these terms that are separately negotiated between CCG and Customer shall be documented in a separate written agreement that shall be deemed Confidential Information of CCG and shall not be disclosed to any third party without the prior written consent of CCG. Unless expressly accepted in writing by Canfield CyberDefense Group, additional or differing terms or conditions proposed by Customer or included in Customer’s acknowledgement are objected to by Canfield CyberDefense Group and have no effect.
2. DEFINITIONS & CONSTRUCTION.
	1. “AdminCore” means the hardware AdminCore 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 On-Premises License, or (ii) for end users who entered into CCG’s Cloud-Based License, the AdminCore resides at CCG’s authorized facilities.
	2. “Affiliated Company” means an entity which directly or indirectly controls or is controlled by Customer. Control is deemed to exist when an entity has the direct or indirect possession of the power to direct the management and policies of another entity.
	3. “Agreement” means this Cyber Security Appliance and Services Agreement and the Related Documents.
	4. “Appliance” means all of CCG’s hardware components for the AdminCore and the Sensor(s). The “AdminCore Appliance” is the hardware components for the AdminCore; the “Sensor Appliance” is the hardware components for the Sensor.
	5. “CCG Technology” means the Appliance, Cyber Security Appliance, Security Solutions, and Documentation, each individually, in any combination, or together.
	6. “CCG Website” means the URL [www.phen-ai.com](http://www.phen-ai.com) and [www.canfieldcyber.com](http://www.canfieldcyber.com), which are comprised of various web pages, tools, information, software, content, and features operated by or on behalf of CCG, and are the intellectual property of CCG.
	7. “Confidential Information” means (i) 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, and (ii) any separately negotiated terms, modifications, or amendments to this Agreement between CCG and Customer that are not part of the standard online terms.
	8. “Customer” means the party identified in the purchase order that is licensing the Cyber Security Appliance and Services from CCG.
	9. “Cyber Security Appliance” means the hardware and software components of the AdminCore and the Sensors.
		1. “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 solution for (i) detecting network problems and insider threats, (ii) providing threat hunting and behavioral analytic detections, scanning, and complete visibility of the network, (iii) monitoring, (iv) providing security and threat analysis, and (v) providing the artificial intelligence functions for CheckMate and Phen.AI.
		2. “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 solution for (i) detecting network problems and insider threats, (ii) providing threat hunting and behavioral analytic detections, including penetration testing, scanning, and complete visibility of the network, (iii) monitoring, (iv) providing security and threat analysis, (v) taking appropriate action, and (vi) providing the artificial intelligence functions for CheckMate and Phen.AI.
	10. “Documentation” means the program documentation, user manuals, handbooks, and other materials describing the use, installation, operation, and maintenance of the Cyber Security Appliance and their Updates, whether distributed or made available as printed materials or as “online” or electronic media.
	11. “Effective Date” means The date that CCG accepts the purchase order for the Cyber Security Appliance and Services.
	12. “EULA” means CCG’s End-User License Agreement, as updated from time to time, located at <https://www.canfieldcyber.com/checkmate>.
	13. “IP Rights” means the intellectual property rights, including copyrights, patents, patents pending, trade secrets, trademarks, and other proprietary rights that are embodied in 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.
	14. “License Term” means the period of time that Customer is 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.
	15. “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”), interfaces, devices, and 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, interfaces, devices, or endpoints, based on the license fee paid and renewal license fee paid, for the License Term.
	16. “Related Documents” means the documents incorporated by reference into this Agreement, including: (i) any purchase orders, task orders, or other instruments issued to authorize deliveries or services under this Agreement; (ii) all documents expressly referenced or linked herein as set forth under “Exhibits and Incorporated Documents” below, including but not limited to the End User License Agreement (EULA), Product Descriptions, Price, Payment, and Delivery Terms, Service Level Polices, Price List, and Terms of Use (TOU); and (iii) any amendments, updates, or successor documents thereto.
	17. “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 AdminCore Appliance and the Sensor Appliance, which together comprise the Cyber Security Appliance, that permit Customer to interact with CheckMate and Phen.AI.
	18. “Sensor” means the components of the Security Solutions that reside on the hardware Sensor Appliance provided by CCG, and which collect and provide data to the AdminCore for monitoring, analysis, and action.
	19. “Service” means the annual services Customer receives for a fee from CCG under the Service Level Policies and limited to those services selected by Customer under the current Price List, which is available through the link to the Price List under Exhibits and Incorporated Documents. Service may include without limitation, telephone setup and configuration, on-site setup and configuration, telephone or on-site support services, bug fixes, updates, upgrades, training, and such other additional services offered by CCG, subject to CCG’s annual services price as provided under the Price List.
	20. “Service Level Policies” means the services level polices of CCG made available to Customer for the fees provided under the policies, which is made available through the link under Exhibits and Incorporated Documents for the Service Level Policies.
	21. “Site” means the location specified in the purchase order for the delivery and installation of the Cyber Security Appliance and each of its components, and for the delivery of those Services selected as part of the purchase order.
	22. “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 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) upgrades, updates, patches, additions, and modifications to the products referred to as CheckMate and Phen.AI.
	23. “TOU” means CCG’s Terms of Use, as updated from time to time, and located at <https://www.canfieldcyber.com/terms-of-use/>.
	24. Headings. The headings in this Agreement are for convenience and will not be used to interpret this Agreement.
	25. Gender and Number. Words in any gender shall be deemed to include all genders, and words denoting number shall include both singular and plural, unless the context otherwise requires.
3. LICENSE GRANT. Subject to the receipt of payment of the annual license fee, support service fees, and compliance with the terms of this Agreement, the EULA, and TOU, the license granted to utilize the Cyber Security Appliance is a non-exclusive, non-transferable, non-sublicensable, revokable, limited license, for a one-year term. The license to continue to utilize the Cyber Security Appliance for each additional one-year term, is subject to receipt of payment of each annual renewal license fee and support service fees prior to the end of the then-current one-year term and the continued compliance with the terms of this Agreement, the EULA (as may be amended from time to time), and TOU (as may be amended from time to time).
	1. On-Premises License. The On-Premises License for the On-Premises Cyber Security Appliance permits the installation and use of the On-Premises Cyber Security Appliance at the Site for providing the selected cyber defenses for the Permitted Number of Interfaces, for Customer’s internal production purposes.
	2. Cloud-Based License. The Cloud-Based License for the Cloud-Based Cyber Security Appliance permits the installation and use of the Sensor(s) at the Site with access to the AdminCore at CCG’s authorized facilities for providing the selected cyber defenses for the Permitted Number of Interfaces, for Customer’s internal production purposes.
	3. Restrictions. Notwithstanding anything to the contrary, this license grant is subject to all restrictions in the EULA, which in summary include without limitation, (i) no copying or creating backup copies of the Security Solutions or Documentation, except as explicitly authorized in writing by CCG, and no copying or distributing of the Security Solutions onto another user’s computer (ii) no permission to permit third-party use or transfer to third-party, (iii) no concurrent use on other computers or devices, unless additional license fee is paid, (iv) no permission to monitor more than the Permitted Number of Interfaces, (v) no other server or network use of the Cyber Security Appliance, AdminCore Appliance, or Sensor Appliance, either directly, through commands, data, or instructions from or to another computer or network, (vi) no removal of proprietary notices, (vii) no export in violation of United States International Traffic in Arms Regulations (“ITAR”), or other applicable regulations, (viii) no modification or creation of derivative works, (ix) no reverse engineering, disassembling or otherwise attempting to discover the source code or underlying ideas or algorithms, (x) no installation of other software on the Appliance, AdminCore Appliance, or Sensor Appliance, or break-down or disassembly of any part of the Appliance, AdminCore Appliance, or Sensor Appliance, or their components, or removal of any tamper-indicating seals, (xi) no training of large language models or artificial intelligence systems, or (xii) no disclosure of any testing or benchmarking results to any third party without CCG’s prior written consent.
	4. Retention of Rights. CCG retains all rights not expressly granted to Customer.
	5. Ambiguity. In the event of ambiguity in the license terms between this Agreement, the EULA, TOU, or other Exhibits, such ambiguity shall be resolved in favor of CCG’s interpretation and the more restrictive interpretation of the license rights and license restrictions as applicable to the Licensee shall apply.
	6. Start. The License Term shall commence on the date of activation of the license key during the build process at CCG’s facilities.
4. THIRD-PARTY LICENSES. CCG does not provide any third-party software and licenses, and it is Customer’s responsibility to obtain any third-party software and licenses on the terms of such licenses and subject to the terms of such third-party license provider, obtain confirmation in writing from CCG that such third-party software (including without limitation, the version of or any modifications to such third-party software) is compatible with CCG’s On-Site Cyber Security Appliance or Cloud-Based Cyber Security Appliance, as appropriate, and pay such licensing fees as required by such third-party licensors prior to CCG’s obligation to provide the Cyber Security Appliances. CCG shall have no liability or responsibility for any issues, defects, failures, or incompatibilities arising from or related to any third-party software or licenses, including but not limited to any impact on the performance or operation of the Cyber Security Appliances or Services.
5. SERVICES.
	1. Platinum Support. Where Customer has an On-Premises License, Customer is obligated to enter into an agreement for CCG’s Platinum Support under CCG’s then-current Service Level Policies for each Security Solution that Customer licenses. Where Customer has a Cloud-Based License, Customer will be obligated to enter into CCG’s support services for CCG’s Standard Support under CCG’s then-current Service Level Policies, or such other support services as determined by the parties.
	2. Additional Services. Customer may obtain additional services under separate agreements for (i) CCG’s Quick Start Services, (ii) Installation Services, (iii) Training Services, (iv) Security Consulting Services, (v) Professional Services, and (vi) such other services offered by CCG, each under CCG’s then-current pricelist.
6. TERM, TERMINATION, AND RETURN.
	1. Term. The obligations under this Agreement shall commence on the Effective Date, provided however the License Term shall commence upon the date of activation of the license key and the License Term shall continue for an initial term of one (1) year (the “Term”) from the date of activation of the license key. Thereafter, this Agreement shall automatically renew for additional one (1) year Terms on the anniversary date on which the license key was activated, unless either party provides written notice of its intent to terminate this Agreement at least forty-five (45) days before the anniversary date of the then-current Term. Prior to each renewal, Customer must review the then-current version of this Agreement at <https://docs.cancgroup.com/partner-nw/agreements>, as the updated terms will apply to the renewal Term. Any renewal shall be at CCG's then-current rates, which shall be provided to Customer at least sixty (60) days prior to renewal.
	2. Termination. This Agreement and any updates or modifications thereto shall be made available at <https://docs.cancgroup.com/partner-nw/agreements>. Notwithstanding anything to the contrary in Section 6.A., CCG may terminate this Agreement or suspend Customer’s access to the Security Solutions, without liability, in the event that:
		1. Failure to Pay Licensing or Support Fee. Customer fails to pay the annual licensing fees, annual renewal license fees, or annual support fees, specified under the then-current price list. Prior to any renewal, Customer must review the then-current version of this Agreement available at <https://docs.cancgroup.com/partner-nw/agreements> as terms may have been updated. Customer's payment of renewal license and support fees constitutes acceptance of any updated terms.
		2. Permitted Number of Interfaces. Customer exceeds the Permitted Number of Interfaces, CCG will provide Customer with written notice of breach. Customer may cure such defects by paying for any additional licensing fees to increase the Permitted Number of Interfaces, or discontinue the use of any non-permitted interfaces. In the event that Customer violates this section more than two times during any given Term, CCG may terminate this Agreement with two (2) days’ written notice, without liability.
		3. IP Rights. Customer breaches any of the terms under Section 9, Confidentiality and Intellectual Property Rights, of this Agreement, in addition to CCG’s right to seek an injunction without the requirement to post bond, CCG may terminate this Agreement immediately.
		4. Insolvency. Customer files for protection under the bankruptcy laws, makes an assignment for the benefit of creditors, appoints or suffers appointment of a receiver or trustee over its property, files a petition under any bankruptcy or insolvency act or has any such petition filed against it which is not discharged within sixty (60) days of the filing thereof, then CCG may terminate this Agreement effective immediately upon written notice to Customer.
	3. Breach of Other Terms. Except as otherwise provided under Section 6.B, in the event Customer breaches any of the other terms of this Agreement, CCG may terminate this Agreement with thirty (30) days’ notice to Customer, unless Customer cures such defect within such thirty (30) day period of time, and notifies CCG in writing within such thirty (30) day period that the breach has been cured.
	4. Post-Termination Rights and Obligations.

* + 1. Transition Assistance. Customer acknowledges that transition assistance or data migration (“Transition Assistance”) is not required from or provided by CCG. However, should Customer seek Transition Assistance upon termination or expiration of the license, Customer shall at least sixty (60) days prior to the termination or expiration of the license, request a price quote from CCG for such services, provided that Customer specify the specific Transition Assistance that Customer requires. If CCG elects to provide such Transition Assistance in its sole discretion, CCG may provide a quote for such services.
		2. Acceleration. The due date of all outstanding invoices for the Cyber Security Appliances, Sensors, and Security Solutions shall automatically accelerate so that they become due and payable on the effective date of the termination, even if longer terms had been previously provided. All orders or portions thereof remaining unshipped as of the effective date of the termination shall automatically be cancelled.
		3. Classified Locations, Destruction. For classified government locations, upon termination of this Agreement for any reason, Customer will cease to utilize the Cyber Security Appliance, Sensors, and Security Solutions. Customer shall, destroy and dispose of the hard drives, the Cyber Security Appliance, Documentation, and any components of CCG’s AdminCore and Sensors, and uninstall and delete any copies of the Security Solutions on Customer’s computers or network. Customer shall provide written certification of the uninstallation and deletion of the Security Solutions, and the destruction of the Cyber Security Appliance, Documentation. and any components of CCG’s AdminCore and Sensors, to CCG.
		4. Other Locations, Return. For all locations other than classified government locations, upon termination of this Agreement for any reason, Customer will cease to utilize the Cyber Security Appliance, Sensors, and Security Solutions, and return all Cyber Security Appliances, Sensors, and Documentation, to CCG, and uninstall and delete any copies of the Security Solutions on Customer’s computers or network. Customer shall provide written certification of the uninstallation and deletion of the Security Solutions to CCG.
		5. Customer Obligation to Delete Data. Prior to returning the Cyber Security Appliances and Sensors to CCG, it is Customer’s obligation, and Customer agrees and covenants to delete all Customer data from the Cyber Security Appliances and Sensors using secure erasure procedures. CCG shall not be responsible for Customer’s data on the returned Cyber Security Appliances or Sensors.
		6. Shipping Costs. Postage will be prepaid by Customer and the tracking number provided to CCG.
		7. Payment for Failure to Return. In the event, Customer fails to return the Cyber Security Appliances or Sensors within thirty (30) days of termination of this Agreement, Customer will be obligated to pay CCG for the cost of the Appliances, AdminCore Appliances, and Senor Appliances, as applicable, and Customer covenants and agrees to pay CCG for the cost of the Appliances, AdminCore Appliances, and Senor Appliances, as applicable, if Customer fails to return the Cyber Security Appliances, AdminCore Appliances, and Sensor Appliances, as applicable, within thirty (30) days.
		8. Lockout Rights. In addition to the obligation to pay CCG under Section 6.D.vii, in the event Customer fails to return the Cyber Security Appliances, AdminCore Appliances, or Sensor Appliances, as applicable, within thirty (30) days of termination of this Agreement for any reason, CCG will have the right, at its sole discretion, to remotely disable, lock, or otherwise prevent Customer’s access to or use of any Cyber Security Appliances, AdminCore Appliances, and Sensor Appliances not returned within thirty (30) days, including electronically locking out Customer from the Cyber Security Appliances, AdminCore Appliances, and Sensor Appliances, as applicable, and from any copy of the Security Solutions installed on any device.
	1. Surviving Provisions. Notwithstanding the termination of this Agreement, the following provisions shall survive and remain in full force and effect: (i) Section 9 (“Confidentiality and Intellectual Property Rights”); (ii) Section 13 (“Indemnification”); (iii) Section 17 (“Dispute Resolution”); and (iv) any other provisions which by their nature are intended to survive termination.
1. PAYMENT TERMS. Customer agrees to pay CCG the amounts specified under this Agreement.
	1. Purchase Order or Invoice. Customer shall provide CCG with a valid purchase order in order for CCG to provide the Cyber Security Appliances, Sensors, or Services; no purchase order shall be binding on CCG until accepted by CCG and payment has been received by CCG. All purchase orders shall be subject to the terms of this Agreement, except as otherwise agreed in writing. Where CCG submits an invoice for the Cyber Security Appliances, Sensors, or Services, Customer shall pay the invoice by the invoice due date; CCG shall not be obligated to provide the Cyber Security Appliances, Sensors, or Services until payment is received.
	2. Payments.
		1. With respect to the Appliances, AdminCore Appliances, or Sensor Appliances, Customer agrees to pay CCG within ten (10) calendar days of the invoice date for the total number of Appliances AdminCore Appliances, or Sensor Appliances ordered, prior to any obligation on the part of CCG to provide the Cyber Security Appliances or Sensors to Customer. All payments are non-refundable.
		2. In the event of late payment, interest shall accrue on any overdue amounts at a rate of 1.5% per month (18% per annum), calculated daily from the due date until the date of payment. This rate applies to all overdue balances following the invoice due date. The Customer explicitly acknowledges and agrees to this interest rate and the conditions under which it is applied.
		3. The interest rate is intended to comply with all applicable laws and regulations and is not intended to be punitive. This interest charge is in addition to any other remedies available to CCG under this Agreement. Customer shall also reimburse CCG for all reasonable costs of collection incurred, including attorney's fees.
	3. UCC-1 Filings. Customer understands that CCG may file a UCC-1 statement (or equivalent filings if outside the United States) with the relevant agency to ensure protection of its Security Solutions and Appliances. Customer authorizes the filing of the UCC-1 statement (or equivalent filings), as well as any addenda. Customer will cooperate with CCG in CCG’s efforts to perfect its title in any filing of UCC-1 statements (or equivalent filings) and any addenda, including providing CCG with the legal name as recorded in the Secretary of State’s office (or equivalent foreign agency) for the business entity.
	4. Taxes. All payments due hereunder are exclusive of all sales taxes, use taxes, value added taxes and any other similar taxes imposed by any federal, state, provincial, or local governmental entity on the transactions contemplated by this Agreement. Except for taxes based on CCG’s income, Customer shall pay any federal, state, local, and foreign taxes, fees or duties imposed on the sale, import, export, use or possession of the Cyber Security Appliances or Services, including penalties and interest. Customer will promptly pay to CCG an amount equal to any such items actually paid or required to be collected and paid by CCG. Customer agrees to pay directly or reimburse CCG (or the authorized distributor, as applicable) for any taxes (including, sales or excise taxes, value added taxes, landing fees, import duties and the like), however designated and whether foreign or domestic, arising out of this Agreement, or CCG’s performance under this Agreement. Customer agrees to pay invoices under this Agreement without deducting any present or future taxes, withholdings or other charges except those deductions it is legally required to make. If Customer is legally required to make any deductions, Customer agrees to pay such amounts as are necessary to make the net amounts remaining after such deductions equal to the stated amount due under this Agreement. The payments or reimbursements will be in such amounts as are sufficient to relieve CCG (or the authorized distributor, as applicable) from owing any further taxes, either directly or on the basis of the payments made under this Agreement. Notwithstanding the foregoing, CCG will be solely responsible for its income tax obligations and all employer reporting and payment obligations with respect to its personnel. Customer agrees to pay any interest and penalties imposed by any taxing authorities to the extent such interest and penalties are applicable to taxes not paid at Customer’s request or as a result of reliance by CCG (or the authorized dealer, as applicable) on Customer’s representations. If a certificate of exemption or similar document or proceeding is necessary in order to exempt any transaction from a tax, Customer will obtain such certificate or document and provide CCG with a copy of such certificate.
2. DELIVERY OBLIGATIONS.

* 1. Shipping. CCG will ship the Cyber Security Appliances to Customer’s Site FOB shipping point. Risk of loss transfers to Customer upon delivery to the carrier. Customer shall be responsible for insurance during transit unless otherwise agreed in writing.
	2. Inspection. Customer agrees that it will immediately inspect the packages prior to acceptance of the Cyber Security Appliances from the delivery company, and contact CCG immediately in the event of damage to the Cyber Security Appliances.
	3. Non-operation.
		1. Within twenty-four (24) hours of acceptance of the Cyber Security Appliance from the delivery company, Customer must contact CCG by email and schedule the set-up and installation of the Cyber Security Appliance, which shall be scheduled to occur within five (5) days of acceptance of the Cyber Security Appliance from the delivery company.
		2. On the date and time scheduled for the set-up and installation of the Cyber Security Appliance, Customer shall contact CCG and CCG shall confirm if the set-up and installation has been successful. Where Customer has elected to utilize CCG’s on-site installation services, CCG will confirm the setup and installation of the Cyber Security Appliance.
	4. Conformity. Except in the case of damage during shipment where Customer has contacted CCG prior to acceptance of the shipment, the parties agree that Customer waives its right to reject the Cyber Security Appliances in the event that Customer believes the Cyber Security Appliances are nonconforming for any reason. In that event, Customer shall contact CCG, and the parties shall seek to resolve any conflict.
	5. Cloud-Based. Where Customer has elected a Cloud-Based Cyber Security Appliance, CCG shall ship only the Sensor(s) to Customer’s Site. Customer agrees to immediately inspect the packages prior to accepting the Sensors from the delivery company, and contact CCG immediately in the event of damage to the Sensors. Customer shall plug the Sensors into the network at the Site within five (5) days of delivery of the Sensor, and promptly contact CCG in the event the Sensors are non-operational upon deployment. Except in the case of damage during shipment where Customer has contacted CCG prior to acceptance of the shipment, the parties agree that Customer waives its right to reject the Sensors in the event that Customer believes the Sensors are nonconforming for any reason. In that event, Customer shall contact CCG, and the parties shall seek to resolve any conflict.
	6. Government. Where Customer is a federal government agency, the delivery obligations will be as agreed upon by the parties in writing.
1. CONFIDENTIALITY AND INTELLECTUAL PROPERTY RIGHTS.
	1. Confidentiality of Negotiated Terms. Any modifications, amendments, or special terms negotiated between CCG and Customer that differ from the standard terms published online shall be deemed CCG's Confidential Information and shall not be disclosed to any third party without CCG's prior written consent.
	2. End User License Agreement. Customer’s use of the Cyber Security Appliance and Security Solutions is explicitly conditioned on Customer’s acceptance of the terms of the EULA. By executing this Agreement, Customer acknowledges its obligation, and covenants to comply with the terms of the EULA. Customer agrees that it may not install or use any Cyber Security Appliance, Sensor(s), Security Solutions, or Documentation, unless Customer agrees to the terms of the EULA.
	3. Customer’s Covenants. Customer covenants and agrees that:
		1. Customer will not make any copies or backup copies of the Security Solutions or Documentation, except as explicitly authorized in writing by CCG, and will not permit the Security Solutions to be copied onto or distributed to another user’s computer.
		2. Customer will not use the Security Solutions for timesharing or service bureau purposes, distribute or otherwise provide the Security Solutions for use by the public or third parties, or transfer the rights in the Security Solutions to a third-party.
		3. Customer will not share or concurrently use the Cyber Security Appliance or Security Solutions on different computers, unless an additional license fee for such use is paid.
		4. Customer will not monitor more than the Permitted Number of Interfaces, IPs, or devices, unless an additional license fee for such use is paid.
		5. Customer will not permit any other server or network to use the Cyber Security Appliance either directly or through commands, data, or instructions from another computer or network, or for Internet or web hosting services.
		6. The Software contains the IP Rights of CCG or its third-party licensors and Customer will not disclose or use the Software except as expressly authorized under this Agreement.
		7. The Software contains copyrighted material, trade secrets, patents, patents pending, and proprietary information owned by CCG or its third-party licensors.
		8. Customer is not authorized to, and will not, modify, de-compile, reverse engineer, disassemble, attempt to discover any source code or underlying ideas or algorithms of the Software, reduce the Software to a human readable form, modify, or create derivate works, of or from the Software.
		9. Customer will not, break-down, open, replace parts, remove drives, or disassemble the Appliances or any components of the Appliances.
		10. Customer will not, rent, lease, loan, use for timesharing or service bureau purposes, reproduce, sublicense or distribute copies of the Software, or otherwise transfer the Software to any third party.
		11. Customer will not remove or alter any trademark, trade name, copyright or other proprietary notices, legends, symbols, or labels appearing on or in copies of the Software.
		12. Customer is not granted any title or rights of ownership in the Appliance, Security Solutions, or Cyber Security Appliance.
		13. The right to use the Appliance, Cyber Security Appliance, and Security Solutions is a license and is not a sale of intellectual property and CCG or its third party licensors continue to own all right, title and interest, including all copyright, patent, patents pending, trademark, trade secret, and moral rights, to the Software, Appliances, and related Documentation, as well as to any corrections, updates and upgrades to it.
		14. The Appliance, Cyber Security Appliance, Security Solutions, and Documentation may be used only in the United States. Any export or transfer of the Appliance, Cyber Security Appliance, Security Solutions, or Documentation outside the United States is strictly prohibited and may violate U.S. export control laws.
	4. Limited Use. Customer agrees to use the Appliance, Cyber Security Appliance, Security Solutions, and Documentation only with CCG’s licensed Security Solutions for active detection and mitigation of cybersecurity threats, and for no other purpose.
	5. Website. 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 licensors. All title and intellectual property rights in and to the information and content which may be accessed through use of the CCG Websites are the property of the respective content owner and may be protected by applicable copyright or other intellectual property laws and treaties.
	6. Injunction. Customer covenants and agrees that any unauthorized use or disclosure of the Confidential Information, or any threat thereof, would likely cause CCG irreparable harm that could not be fully remedied by monetary damages. Thus, Customer agrees that CCG will have the right, in addition to any other remedy available to it, to seek injunctive or other equitable relief from a court of competent jurisdiction, without proof of actual damage, and without posting bond, as may be necessary to prevent any unauthorized use or disclosure of CCG’s Confidential Information.
2. CHANGES TO CYBERSECURITY MONITORING.
	1. Check-in. The Software is required to check-in electronically with the CCG Website once every twenty-four- hour period. If the Software fails to check-in with the CCG Website, the Software may fail to update with the latest bug fixes, patches, or updates.
	2. Maintenance and Emergency Updates. CCG and its suppliers reserve the right, at any time, with or without prior notice to Customer, to restrict or suspend the functionality of the Software to perform maintenance activities and to maintain session control. In the event of critical security vulnerabilities or other emergencies requiring immediate updates, CCG will make commercially reasonable efforts to notify the Customer. CCG reserves the right to implement emergency security updates immediately without prior approval if CCG determines, in its sole discretion, that such updates are necessary to protect the system's integrity or prevent potential security breaches.
	3. Service or Features. CCG reserves the right to change any of the features, content, or devices authorized by CCG for use in connection with the cybersecurity monitoring functions or other functions of the Software, at any time with or without notice to Customer.
	4. Remote Updates. CCG reserves the right to periodically update, upgrade, change, or add new Security Solutions remotely or otherwise and to make related changes to the settings and software on the Appliance, or any device authorized by CCG for use in connection with the Security Solutions, and Customer agrees to permit such changes and access to Customer’s computer, the Appliances, and any such device authorized by CCG for use in connection with the Security Solutions.
	5. Updated EULA and TOU. CCG reserves the right to periodically update, change, or revise this Agreement, EULA, and TOU. The most current version of this Agreement will be available at <https://docs.cancgroup.com/partner-nw/agreements>. Prior to any renewal term, Customer must review the then-current Agreement, EULA, and TOU. Customer’s payment for and continued use of the Cyber Security Appliance, Security Solutions, or Services in any renewal term constitutes acceptance of the then-current Agreement, EULA, and TOU. If Customer does not agree to the updated Agreement, EULA, or TOU, Customer must notify CCG prior to the renewal term and cease using the Cyber Security Appliance, Software, and Services. Customer acknowledges that the EULA and TOU may be updated from time to time during the licensed period, and that Customer’s continued use of the Cyber Security Appliance, Security Solutions, or Services, constitutes acceptance of the EULA and TOU during the licensed period; in the event Customer objects to any of the updated provisions of the EULA or TOU, Customer shall immediately contact CCG to notify CCG of its objections, and either resolve the issue and continue using the Cyber Security Appliance, Security Solutions, or Services, or cease use of the Cyber Security Appliance, Security Solutions, and Services, as determined by the parties; but in no event, shall Customer be entitled to renew the license period at the next renewal period where Customer has not agreed to the then-current terms of the EULA or TOU.
3. CUSTOMER’S ACKNOWLEDGEMENT, REPRESENTATION, AND WARRANTY.
	1. Legal Authority. Customer represents and warrants that Customer has the legal authority to enter into this Agreement, that it is duly authorized and empowered to execute, deliver and perform this Agreement and that such action does not conflict with or violate any provision of law, regulation, policy, contract, or other instrument to which it is a party or by which it is bound, and that this Agreement constitutes a valid and binding obligation enforceable in accordance with its terms.
	2. Monitoring. Customer acknowledges that Customer is responsible for all use of the Software and Appliances and for monitoring the data provided by the Appliance.
	3. Compliance. Customer agrees to comply with all applicable laws, regulations and rules regarding Customer’s use of the Appliance and Software and to only use the Appliance and Software within the United States (unless otherwise permitted by this Agreement).
	4. Restrictions on Use. Customer agrees that it will not sell, resell, re-provision, or rent the Security Solutions or any of its components, (either for a fee or without charge) or allow third parties to use the Security Solutions via wired, wireless, or other means, except as otherwise explicitly agreed by CCG in writing.
4. WARRANTIES AND LIMITATION OF LIABILITY.
	1. Infringement Warranty. If any Security Solutions furnished under this Agreement becomes, or in CCG’s reasonable opinion is likely to become, the subject of any claim, suit, or proceeding arising from or alleging infringement of any intellectual property rights, CCG, at its own expense, shall take any of the following actions, in CCG’s discretion:
		1. Secure for Customer the right to continue using the Security Solutions;
		2. Replace or modify the Security Solutions to make it non-infringing;
		3. Direct Customer to stop using the Security Solutions and refund a maximum of up to six (6) months of Customer’s software license fees (but excluding all other fees, including hardware fees, nonrecurring charges, regulatory fees, surcharges, service fees, and taxes) for its then-current valid license period. CCG will not be responsible for any infringing use that Customer may make of the Security Solutions after CCG directs Customer to stop using the Software.
	2. Limited Warranty. CCG provides a limited warranty for a period of 30 days from the date of activation of the License Key. CCG warrants that when properly installed and used under normal conditions, the Security Solutions, and where applicable, the Appliance, will perform substantially in accordance with the Documentation. If the Security Solutions, and where applicable, the Appliance, does not perform substantially in accordance with the Documentation, the entire and exclusive liability of CCG and its distributors and agents and Customer’s sole and exclusive remedy will be limited to replacement of the Security Solutions, and where applicable, the Appliance.
	3. SERVICES. **ALL SERVICES, MATERIALS, OR OTHER INFORMATION PROVIDED BY CCG UNDER THIS AGREEMENT ARE FURNISHED ON AN “AS-IS” BASIS. CCG MAKES NO EXPRESS, IMPLIED OR STATUTORY WARRANTIES, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ANY IMPLIED WARRANTIES ARISING FROM STATUTE, COURSE OF DEALING, COURSE OF PERFORMANCE OR USAGE OF TRADE. CCG MAKES NO WARRANTY AS TO ANY RESULTS TO BE ATTAINED BY RECEIVING THE SERVICES OR USING THE MATERIALS PROVIDED HEREUNDER.**
	4. SOFTWARE, APPLIANCE, AND DOCUMENTATION. **CCG (AND ITS OFFICERS, EMPLOYEES, PARENT, SUBSIDIARIES, AND AFFILIATES) (COLLECTIVELY THE "CCG PARTIES"), ITS THIRD-PARTY LICENSORS, PROVIDERS AND SUPPLIERS (COLLECTIVELY, THE “THIRD-PARTY LICENSORS”), DISCLAIM ANY AND ALL WARRANTIES AND CONDITIONS FOR THE CYBER SECURITY APPLIANCE, APPLIANCE, SENSORS, SECURITY SOLUTIONS, SOFTWARE, AND DOCUMENTATION, WHETHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ACCURACY, NON-INFRINGEMENT, NON-INTERFERENCE, TITLE, COMPATIBILITY OF COMPUTER SYSTEMS, COMPATIBILITY OF SOFTWARE PROGRAMS, INTEGRATION, AND THOSE ARISING FROM COURSE OF DEALING, COURSE OF TRADE, OR ARISING UNDER STATUTE. FURTHER, THERE IS NO WARRANTY OF WORKMANLIKE EFFORT OR LACK OF NEGLIGENCE. NO ADVICE OR INFORMATION GIVEN BY THE CCG PARTIES, OR THE THIRD-PARTY LICENSORS, SHALL CREATE A WARRANTY WITH RESPECT TO ADVICE PROVIDED.**
	5. NO LIABILITY. **IN NO EVENT SHALL THE CCG PARTIES OR CCG'S THIRD PARTY LICENSORS BE LIABLE FOR: (A) ANY DIRECT, INDIRECT, PUNITIVE, SPECIAL, CONSEQUENTIAL OR INCIDENTAL DAMAGES, INCLUDING LOST PROFITS OR LOSS OF REVENUE, LOSS OF PROGRAMS OR INFORMATION OR DAMAGE TO DATA ARISING OUT OF THE USE, PARTIAL USE OR INABILITY TO USE THE CYBER SECURITY APPLIANCES, APPLIANCES, SENSORS, SECURITY SOLUTIONS, SOFTWARE, OR DOCUMENTATION, OR RELIANCE ON OR PERFORMANCE OF THE AFOREMENTIONED, 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 CCG HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH CLAIM OR DAMAGES, OR (B) ANY CLAIMS AGAINST CUSTOMER BY ANY OTHER PARTY. CUSTOMER ACKNOWLEDGES AND AGREES THAT THIS LIMITATION OF LIABILITY APPLIES TO FAILURES OF THIRD-PARTY COMPONENTS THAT MAY IMPACT SERVICE DELIVERY, AND CUSTOMER ASSUMES ALL RISKS ASSOCIATED WITH THIRD-PARTY COMPONENT FAILURES AND THEIR IMPACT ON SERVICE DELIVERY.**
	6. PERFORMANCE. **CCG AND ITS RESELLERS, DEALERS, DISTRIBUTORS, AND AGENTS DO NOT WARRANT THE PERFORMANCE OR RESULTS CUSTOMER MAY OBTAIN BY USING ANY CYBER SECURITY APPLIANCES, APPLIANCES, SENSORS, SECURITY SOLUTIONS, SOFTWARE, OR DOCUMENTATION. CCG DOES NOT WARRANT THAT THE OPERATION OF THE AFOREMENTIONED WILL BE UNINTERRUPTED OR ERROR FREE, THAT THE AFOREMENTIONED WILL WORK PROPERLY ON ANY GIVEN DEVICE OR WITH ANY PARTICULAR CONFIGURATION OF APPLIANCES, SENSORS, OR SECURITY SOLUTIONS, OR THAT THE SECURITY SOLUTIONS, CYBER SECURITY APPLIANCES OR SENSORS, WILL PROVIDE COMPLETE PROTECTION FOR THE INTEGRITY OF SELECTED DATA, INFORMATION OR CONTENT STORED OR TRANSMITTED WITHIN CUSTOMER’S NETORK. CCG DOES NOT WARRANT THAT ANY OF THE CYBER SECUIRTY APPLIANCES, SENSORS, SECURITY SOLUTIONS, OR OTHER DEVICES AUTHORIZED BY CCG FOR USE IN CONNECTION WITH THE CYBERSECURITY MONITORING AND DEFENSE WILL PERFORM AT A PARTICULAR SPEED, BANDWIDTH OR DATA THROUGHPUT RATE, OR WILL BE UNINTERRUPTED, ERROR-FREE, SECURE, OR FREE OF VIRUSES, WORMS, DISABLING CODE OR CONDITIONS, OR THE LIKE. CCG SHALL NOT BE LIABLE FOR LOSS OF CUSTOMER’S DATA, OR IF CHANGES IN OPERATION, PROCEDURES, OR SERVICES REQUIRE MODIFICATION OR ALTERATION OF CUSTOMER’S DEVICE (INCLUDING ANY OTHER DEVICE AUTHORIZED BY CCG FOR USE IN CONNECTION WITH CYBERSECURITY MONITORING), RENDER THE SAME OBSOLETE OR OTHERWISE AFFECT ITS PERFORMANCE.**
	7. PROVISIONING. **CCG DOES NOT WARRANT OR GUARANTEE THAT THE SECURITY SOLUTIONS OR APPLIANCE CAN BE PROVISIONED TO CUSTOMER’S LOCATION, OR THAT PROVISIONING WILL OCCUR ACCORDING TO A SPECIFIED SCHEDULE, EVEN IF CCG HAS ACCEPTED CUSTOMER’S PURCHASE ORDER FOR THE APPLIANCE**.
	8. REMEDY. **THE LIABILITY OF THE CCG PARTIES, OR (SUBJECT TO ANY DIFFERENT LIMITATIONS OF LIABILITY IN THIRD PARTY END USER LICENSE OR OTHER AGREEMENTS) THE THIRD-PARTY LICENSORS, FOR ALL CATEGORIES OF DAMAGES SHALL BE LIMITED TO CUSTOMER’S RIGHT TO TERMINATE ANY REMAINING PERIOD OF THE LICENSE AGREEMENT, ANY RENEWAL PERIODS AND UPCOMING PAYMENTS, AND RETURN, AT CUSTOMER’S EXPENSE, THE APPLIANCES, AND UNINSTALL ALL COPIES FO THE SOFTWARE. THE LIABILITY OF THE CCG PARTIES AND THIRD-PARTY LICENSORS SHALL BE LIMITED TO A MAXIMUM OF UP TO THREE (3) MONTHS OF THE SECURITY SOLUTIONS LICENSE FEE (BUT EXCLUDING ALL OTHER FEES, INCLUDING, HARDWARE FEES, NONRECURRING CHARGES, REGULATORY FEES, SURCHARGES, SERVICE FEES AND TAXES), FOR THE THEN-CURRENT VALID LICENSE PERIOD THAT CUSTOMER HAS PAID TO CCG, WHICH SHALL BE CUSTOMER’S SOLE AND EXCLUSIVE REMEDY REGARDLESS OF THE TYPE OF CLAIM OR NATURE OF THE CAUSE OF ACTION. THE FOREGOING LIMITATIONS SHALL APPLY TO THE FULLEST EXTENT PERMITTED BY LAW AND ARE NOT INTENDED TO ASSERT ANY LIMITATIONS OR DEFENSES WHICH ARE PROHIBITED BY LAW. NO REFUND WILL BE DUE WHERE CUSTOMER HAS NOT PAID A LICENSE FEE FOR THE THEN-CURRENT LICENSE PERIOD OF CUSTOMER’S CLAIM.**
	9. BENEFICIARIES. **ALL LIMITATIONS AND DISCLAIMERS STATED IN THIS SECTION 12 ALSO APPLY TO THE THIRD-PARTY LICENSORS, AS THIRD-PARTY BENEFICIARIES OF THIS AGREEMENT.**
	10. EXCLUSIVE REMEDIES. **THE REMEDIES EXPRESSLY SET FORTH IN THIS AGREEMENT ARE CUSTOMER’S SOLE AND EXCLUSIVE REMEDIES.**
5. INDEMNIFICATION. Customer agrees to defend, indemnify and hold harmless the CCG Parties from and against any and all claims, demands, actions, suits, proceedings, liabilities, losses, damages, costs and expenses (including, without limitation, reasonable attorneys' and experts' fees), arising out of or relating to: (a) Customer’s use of the Security Solutions, Appliances, Cyber Security Appliances, or other devices, used in connection with the cybersecurity monitoring and defense (or the use of the Security Solutions, Appliances, Cyber Security Appliances, or any other devices by anyone else, with or without Customer’s permission); (b) any violation of applicable laws, regulations, or this Agreement by Customer or any third party using the Security Solutions, Appliances, Cyber Security Appliances, or other devices; (c) any third-party claims arising from or relating to Customer’s use of the Security Solutions, Appliances, Cyber Security Appliances, or other devices; or (d) 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 property (including without limitation, data).
6. ENTIRE AGREEMENT. This Agreement supersedes any and all other prior understandings and agreements, whether oral or in writing, between the parties with respect to the subject matter in this Agreement and constitutes the sole understanding between the parties with respect to the said subject matter. All prior negotiations and agreements between the parties with respect to the subject matter are merged into this Agreement. Each party to this Agreement acknowledges that no representations, inducements, promises, or agreements, orally or otherwise, have been made by any party or by anyone acting on behalf of any party, which are not embodied in this Agreement and that any agreement, statement or promise that is not contained in this Agreement will not be valid or binding or of any force or effect. If CCG has agreed to any modifications, amendments, or special terms with Customer that differ from the standard terms set forth in this Agreement or the Related Documents, such negotiated terms (the “Negotiated Terms”) are the Confidential Information of CCG and Customer shall not disclose such Negotiated Terms to any third party without CCG's prior written consent, except as required by law or valid legal process. This confidentiality obligation shall survive the termination or expiration of this Agreement.
7. NOTICES. All notices required to be sent shall be sent to the addresses, facsimile numbers, or email addresses provided under Schedule E (or as subsequently updated in writing by either party), and shall be deemed given (i) on the date of receipt, 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 (i), postage or delivery costs shall be prepaid. The addresses, facsimile numbers, or email addresses may be changed by the each of the parties from time to time by providing notice to the then current address, facsimile number, or email address.
8. DURATION. Any terms of this Agreement which by their nature extend beyond expiration or termination of this Agreement shall remain in effect until fulfilled and shall bind the parties and their legal representatives, successors, heirs and assigns. The requirements of Section 9 shall survive any termination of this Agreement.
9. DISPUTE RESOLUTION. In the event of a dispute between the parties, the parties agree to first attempt to resolve the dispute through good faith negotiations for a period of thirty (30) days. If negotiations fail, the parties agree to mediate their dispute with a neutral mediator in Maryland prior to proceeding with any legal action. The costs of mediation shall be shared equally between the parties. This Agreement shall be governed by and construed in accordance with the laws of the State of Maryland, without giving effect to any choice of law principles.

**EXHIBITS AND INCORPORATED DOCUMENTS**

**This Agreement and the following documents are hereby incorporated by reference and made a part of this Agreement. By executing this Agreement or placing a purchase order, Customer acknowledges receipt of or access to these documents and agrees to be bound by their terms. The most current version of this Agreement and all incorporated documents are available at the links provided below:**

1. Appliance and Services Agreement:

 <https://docs.cancgroup.com/partner-nw/agreements>

2. End User License Agreement (EULA):

 <https://www.canfieldcyber.com/checkmate>

3. Terms of Use (TOU):

 <https://www.canfieldcyber.com/terms-of-use>

4. Service Level Policies:

 <https://www.canfieldcyber.com/pricing-options/>

5. Product Descriptions:

 <https://www.canfieldcyber.com/products/>

7. Price List:

SECURE CLOUD PRICING: <https://www.canfieldcyber.com/pricing-options/>

ON PREMISES PRICING: <https://www.canfieldcyber.com/pricing-appliances/>

Version 1.5