Board of County Commissioners Agenda Request

2V
Agenda Item #

Requested Meeting Date: 14 APRIL 2026

Title of Item: MNIT Cybersecurity Services Contract

☐ REGULAR AGENDA	**Action Requested:**	☐ Direction Requested
☑ CONSENT AGENDA	☑ Approve/Deny Motion	☐ Discussion Item
☐ INFORMATION ONLY	☐ Adopt Resolution (attach draft)	☐ Hold Public Hearing*
		**provide copy of hearing notice that was published*

Submitted by: Chris Sutch	**Department:** IT
Presenter (Name and Title): Chris Sutch, IT Manager	**Estimated Time Needed:** 0

Summary of Issue:

Since the Federal Government has de-funded parts of Multi-State Information Sharing and Analysis Center (MS-ISAC) and moved key services to a paid subscription model, I no longer see value in maintaining our membership. The primary service we relied on was MDBR (Malicious Domain Blocking and Reporting). MNIT now provides its own MDBR service at no cost to counties and other Minnesota agencies. Aitkin also continues to use MNIT's free external vulnerability scanning service through their Threat and Vulnerability Management Unit (TVMU).

County Attorney Ratz has reviewed the agreement with the State including the Work Order Contract and find it to be appropriate as to form and content.

Alternatives, Options, Effects on Others/Comments:

Recommended Action/Motion:

Approve motion to allow IT Manager Chris Sutch to approve this contract for free services with MNIT.

Financial Impact:

Is there a cost associated with this request? ☐ *Yes* ☑ *No*

What is the total cost, with tax and shipping? $

Is this budgeted? ☐ *Yes* ☑ *No* *Please Explain:*

Legally binding agreements must have County Attorney approval prior to submission.

Whole-of-State Service Agreement and Work Order Contract

State of Minnesota

Executive Summary

Minnesota IT Services (MNIT), in partnership with the Minnesota Cybersecurity Task Force, launched the Whole-of-State Cybersecurity Plan in 2023 to strengthen local government cyber defenses. The whole-of-state approach presents a strong, united front against cyber threats, and bolsters cybersecurity across Minnesota.

The Cybersecurity Task Force established four goals to advance the Whole-of-State Plan: Mature cyber capabilities throughout the state; collaborate and share information throughout the state; increase participation in programs and services known to work; and strengthen the cyber-resiliency of critical infrastructure. These goals are designed to provide a solid foundation for a long-term, sustainable cybersecurity system that builds on results and moves with the times.

MNIT is creating a framework built on collaboration and inclusion to provide the tools, resources, and information eligible entities need to help secure the data that Minnesotans have entrusted to their organization.

Under the whole-of-state approach, the Statewide Security Monitoring Initiative (SSMI) – also referred to as the State Homeland Security Grant Program (SHSP) - and the State and Local Cybersecurity Program (SLCGP) use funding to create a layered approach to security. This helps protect Minnesotans by advancing stronger, sustainable cybersecurity tools and processes that leverage best practices, build on past successes, meet every organization where they are, educate, and freely share information.

Work Order Contract

This Work Order Contract is between the State of Minnesota, acting through its commissioner of Minnesota IT Services ("State") and Aitkin County ("Governmental Unit"), whose designated business address is 307 2nd St NW, Aitkin MN 56431. "Governmental Unit" includes any agents, employees, or third-party service providers working on behalf of the Governmental Unit.

The Statewide Security Monitoring Initiative (SSMI) is a program devoted to protecting the data of all Minnesotans by partnering with participating county governments, port cities, and Tribal Nations to ultimately fortify the cybersecurity of the entire state of Minnesota. The State and Local Cybersecurity Grant Program (SLCGP) is a program devoted to protecting the technology, data, and systems that make our government and schools run is one of our highest priorities and aims to make sure that our state, county, municipal, and tribal government, education, public health, critical infrastructure, and peacekeepers have all the cybersecurity tools and resources they need.

Governmental Unit is requesting State to provide certain security services through its SSMI and/or SLCGP program as identified in this Work Order Contract.

Contract

1. Term of Work Order

1.1 Effective date. This Work Order is effective on the date State obtains all required signatures under Minn. Stat. § 16C.05, subd. 2. State will not begin work under this contract until this contract is fully executed and State has been notified by Governmental Unit's Authorized Representative to begin work.

1.1 Expiration date. This Work Order is effective through June 30, 2027.

2. Service Selection and Authorization

Upon execution of this Work Order, State will provide the services selected by Governmental Unit in Table 1. Some services are performed only by State ("First-Party Services"). Some services include work performed or tools provided by third parties, either in conjunction with or independent of State's provision of services ("Third-Party Services"). For more information visit **https://mn.gov/mnit/about-mnit/security/wos/.**

SELECTION(S)	SERVICE OFFERING	DESCRIPTION OF SERVICE OFFERING
☑	1 – External Vulnerability Scans	The Minnesota IT Services (MNIT) Threat and Vulnerability Management Unit (TVMU) provides external vulnerability Management service. MNIT provides a comprehensive vulnerability scanning service that utilizes sophisticated and automated vulnerability scanning and attack surface management technology. MNIT continuously monitors scan results, assesses critical and high-risk vulnerabilities, and communicates actionable information to the participating entity. The term of this contract expires on June 30, 2027. More information available here: https://mn.gov/mnit/about-mnit/security/wos/
	2 – Internal Vulnerability Scans	The MNIT Threat and Vulnerability Management Unit (TVMU) provides internal vulnerability management service to SSMI eligible entities. TVMU provides a comprehensive vulnerability scanning tool that utilizes sophisticated enterprise class scanning technology to conduct in-depth vulnerability and configuration compliance scanning using credentials/agents' technology. The TVMU team conduct regular briefing meetings with participating organizations to discuss scan findings and remediation. The term of this contract expires on June 30, 2027. More information available here: https://mn.gov/mnit/about-mnit/security/wos/ Billing is done on a monthly basis, according to the size category the Governmental Unit falls within and the number of addresses scanned. Contact the TVMU team (TVMU@state.mn.us) for more information on Internal Vulnerability Scanning billing.
	3 - SIEM	The Next Generation Security Information and Event Management (SIEM) program is provided at a reduced cost to Minnesota counties, cities, townships, public K12s, Tribal entities, and other partner organizations through the CrowdStrike console. Pricing is based on daily ingest amount and record retention needs. More information available here: https://mn.gov/mnit/about-mnit/security/wos/ The term of this contract expires on June 30, 2027. Billing is done monthly based on data ingest and contracted end-point counts. Billing will be based on monthly usage. Contact the Cyber Navigator team (CN.MNIT@state.mn.us) for more

		information on SIEM billing: https://mn.gov/mnit/about-mnit/security/whole-of-state-cybersecurity-plan/ngs.jsp
	4 – MDR	The Managed Detection and Response (MDR) program is provided at a reduced cost to Minnesota counties, cities, townships, public K12s, Tribal entities, and other partner organizations through the CrowdStrike console. More information available here: https://mn.gov/mnit/about-mnit/security/wos/ The term of this contract expires on June 30, 2027. Governmental Unit agrees to be billed monthly based on the contracted amount specified in this agreement. If the Governmental Unit's usage exceeds the contracted amount, the Governmental Unit will be invoiced for the overage at the rates specified in this agreement. Contact the Cyber Navigator team (CN.MNIT@state.mn.us) for more information on MDR billing.
	5 - EDR	The Endpoint Detection and Response (EDR) program is provided at a reduced cost to Minnesota counties, cities, townships, public K12s, Tribal entities, and other partner organizations. The EDR program does not include oversight and management from CrowdStrike or MNIT. More information available here: https://mn.gov/mnit/about-mnit/security/wos/ The term of this contract expires on June 30, 2027. Governmental Unit agrees to be billed monthly based on the contracted amount specified in this agreement. If the Governmental Unit's usage exceeds the contracted amount, the Governmental Unit will be invoiced for the overage at the rates specified in this agreement. Contact the Cyber Navigator team (CN.MNIT@state.mn.us) for more information on EDR billing.
☑	6 – MDBR	Malicious Domain Blocking and Reporting (MDBR): A cloud-based solution that uses technology to prevent IT systems from connecting to harmful web domains and limit infections related to malware, ransomware, phishing, and other cyber threats. The term of this contract expires on June 30, 2027. For more full program participation rules and more information see website: https://mn.gov/mnit/about-mnit/security/wos/ This is a no charge service. Governmental Unit will not be billed as this service is being covered by the SLCGP grant. For more information, contact the Cyber Navigator team (CN.MNIT@state.mn.us)

Table 1

Governmental unit understands that State is subsidizing some or all these services through a combination of State Homeland Security Grant Program (SHSP) and State and Local Grant Program (SLCGP) funds allocated to Minnesota. This funding includes:

- State and Local Cybersecurity Grant Program for Federal Fiscal Year (FFY) 2023, Funding Opportunity **DHS-23-137-000-01**, as authorized by Section 2220A of Homeland Security Act of 2002, as amended (Pub. L. No. 107-296) (6 U.S.C. § 665g).
- State Homeland Security Grant Program (SHSP) for FFY 2023, Funding Opportunity (**DHS-23-GPD-067-00-01**) as authorized by Section 2002 of the Homeland Security Act of 2002 (Pub. L. No. 107-296, as amended) (6U.S.C. § 603).
- Minnesota State and Local Cybersecurity Grant Program has a State Match requirement for FFY23 **(see** Laws of Minnesota 2023, chapter 62, article 1, section 10**)**.

- For more information on these grants and their allocation, please see the MNIT Whole of State program webpage here: https://mn.gov/mnit/about-mnit/security/wos/

Governmental unit consents and accepts these services in lieu of direct allocation of funds from these grant programs. Governmental unit agrees that it is responsible for subsidized portion in the event these funding sources are no longer available. For more information on these programs, please refer to https://mn.gov/mnit/about-mnit/security/wos/.

Governmental Unit understands and agrees State's provision of services under this Work Order do not include remediation of any security issues identified during State's provision of services.

Governmental Unit understands and agrees that some selected Third-Party Services may require a minimum term commitment ("Minimum Commitment") from Governmental Unit, as identified in Table 1. Governmental Unit agrees to pay for the quantity of services identified in Table 1 with a Minimum Commitment selected for the duration of the Minimum Commitment.

3. Representations and Warranties

3.1 Under Minnesota Statutes Ch. 16E, State is empowered to create and maintain state cyber security systems and ensure overall security of the state's information and technology systems and services; promote cooperation and collaboration among state and local governments in developing intergovernmental information and telecommunications technology systems and services; and enter into contracts with agencies of the federal government, local governmental units, the University of Minnesota and other educational institutions, and private persons and other nongovernmental organizations as necessary to perform its statutory duties.

3.2 Governmental Unit represents and warrants that it possesses the legal authority to enter into this Work Order and that it has taken all actions required by its procedures, by-laws, and applicable laws to exercise that authority, and to lawfully authorize its undersigned signatory to execute this Work Order, or any part thereof, and to bind Governmental Unit to its terms.

4. Consideration and Payment

All service costs and billing considerations are available on https://mn.gov/mnit/about-mnit/security/wos/ or by contacting the Cyber Navigator team (CN.MNIT@state.mn.us) or TVMU team (TVMU@state.mn.us). MNIT will provide 90 days notice before changing the published rates of these programs.

Billing is compiled after the end of each month and invoices are posted within CosWeb (cosweb.mnit.state.mn.us) for Governmental Unit access, under Computing Services. Governmental Unit billing contact(s) will receive an email message notifying them there is at least one new invoice to review.

Internal Vulnerability Scanning billing is based upon the size category assigned to the Governmental Unit as well as the number for addresses requested to be scanned. These address amounts are audited annually.

MDR billing is based upon the number for MDR licenses requested, so will always be at least that number – if more licenses are in use at the end of the month, Governmental Units will be charged for that larger number of licenses.

EDR billing is based upon the number for EDR licenses requested, so will always be at least that number – if more licenses are in use at the end of the month, Governmental Units will be charged for that larger number of licenses.

SIEM billing is based upon the number for SIEM licenses requested, so will always be at least that number – if more licenses are in use at the end of the month, Governmental Units will be charged for that larger number of licenses.

5. Authorized Representatives
State's Authorized Representative, their delegate, or successor in office is required to sign this Work Order.

6. Third Party Terms
Governmental Unit acknowledges it has reviewed the terms of the agreements State has with its third-party contractors used to provide the services selected by Governmental Unit under this Work Order, which are available at https://mn.gov/mnit/about-mnit/security/wos/, as updated. ("Third-Party Terms"). Governmental Unit agrees to comply with the Third-Party Terms to the extent those terms apply to the services ordered and received by Governmental Unit under this Work Order.

7. Assignment, Amendments, Waiver, and Contract Complete.

7.1 Assignment. Neither Party may assign nor transfer any rights or obligations under this Agreement without the prior consent of the other Party and a fully executed assignment agreement, executed and approved by the authorized parties or their successors.

7.2 Amendments. Any amendment to this Agreement must be in writing and will not be effective until it has been executed and approved by the authorized parties or their successors.

7.3 Waiver. If either Party fails to enforce any provision of this Agreement, that failure does not waive the provision or its right to enforce it.

7.4 Contract Complete. This Work Order, including as applicable Third-Party Waivers, Master Control Agreements, and Third-Party Terms incorporated by reference, contains all negotiations and agreements between State and Governmental Unit. No other understanding regarding this Agreement, whether written or oral, may be used to bind either party.

8. Liability.

8.1 Each party will be responsible for its own acts and behavior and the results thereof.

8.2 Nothing within this Agreement, whether express or implied, shall be deemed to create an obligation on the part of State to indemnify, defend, hold harmless or release Governmental Unit. This shall extend to all agreements related to the subject matter of this Contract, and to all terms subsequently added, without regard to order of precedence.

9. State Audits.
Under Minn. Stat. § 16C.05, subd. 5, Governmental Unit's books, records, documents, and accounting procedures and practices relevant to this Agreement are subject to examination by State, the State Auditor, or Legislative Auditor, as appropriate, for a minimum of six years from the expiration or termination of this Agreement.

10. Government Data Practices.
Governmental Unit and State must comply with the Minnesota Government Data Practices Act, Minn. Stat. Ch. 13, (or, if State contracting party is part of the Judicial Branch, with the Rules of Public Access to Records of the

Judicial Branch promulgated by the Minnesota Supreme Court as the same may be amended from time to time) as it applies to all data provided by State under this Agreement, and as it applies to all data created, collected, received, stored, used, maintained, or disseminated by the Governmental Unit under this Contract. The civil remedies of Minn. Stat. § 13.08 apply to the release of the data governed by the Minnesota Government Practices Act, Minn. Stat. Ch. 13, by either Governmental Unit or State.

If the Governmental Unit receives a request to release the data referred to in this clause, Governmental Unit must promptly notify and consult with State's Authorized Representative as to how the Governmental Unit should respond to the request. Governmental Unit's response to the request shall comply with applicable law.

11. Governing Law, Jurisdiction, and Venue.
Minnesota law, without regard to its choice-of-law provisions governs this Work Order. Venue for all legal proceedings out of this Work Order, or its breach, must be in the appropriate state or federal court with competent jurisdiction in Ramsey County, Minnesota.

12. Termination
State or Governmental Unit may terminate this Work Order at any time, with or without cause, upon 60 days written notice to the other Party. Termination will be effective at the end of the month in which the 60 day period concludes. The State will bill through the end of the next closest month following the termination. For Third-Party Services with a Minimum Commitment, Governmental Unit understands and agrees that termination will terminate provision of services, but Governmental Unit will remain obligated to the amounts owed for the Minimum Commitment. This Work Order will terminate automatically upon execution between State and Governmental Unit of a subsequent Work Order covering the same or additional service selections.

13. Renewal

Governmental Unit shall notify State of its desire to enter into a new Work Order for further provision of services within 60 days of the expiration date of this Work Order.

1. **Governmental Unit**
The Governmental Unit certifies that the appropriate person has executed the Work Order Contract on behalf of the Governmental Unit as required by applicable laws, articles, bylaws, resolutions, or ordinances.

Print Name: Chris Sutch

Signature: _____

Title: IT Manager

Date: _____

2. **State Agency**
With delegated authority

Print Name: John Israel

Signature: _____

Title: MNIT CISO Date: _____

3. **Commissioner of Administration**
As delegated to The Office of State Procurement

Print Name: _____

Signature: _____

Title: _____ Date: _____

Admin ID: _____

MINNESOTA IT SERVICES

Liability Release, Waiver, and Agreement for Application Security Assessment

In exchange for Minnesota IT Services ("MNIT") providing endpoint detection and response platform using CrowdStrike ("Scanning"), Governmental Unit represents that:

The Governmental Unit UNDERSTANDS THE NATURE OF THE SCANNING, and that MNIT will be deploying automated and/or manual endpoint detection tools to assist the Governmental Unit in detecting, hunting, and responding to cyber threats, risks, and vulnerabilities within the agency's/Governmental Unit's data environment. The Governmental Unit acknowledges that after MNIT's deployment of the tools, MNIT with assistance from the Governmental Unit Security Team will access the sites/resources provided by the Governmental Unit through automated and/or manual processes to review threats provided by the tool. During the assessment, MNIT along with the Governmental Unit Security Team may access protected content within the specific systems in scope for this assessment. The Governmental Unit understands that MNIT is only providing the security assessment and it is the responsibility of the Governmental Unit to carry out the investigation for and remediation of vulnerabilities identified within the Governmental Unit's data environment. Should The Governmental Unit request additional assistance, MNIT is also able to assist with the assessment of the scanning results and advising on the impact that the vulnerabilities may have on the system. Further, the Governmental Unit acknowledges that the use of MNIT's CrowdStrike tool involves a risk to the Governmental Unit's IT equipment and could also cause an impact to the Governmental Unit services, though the likelihood of being impacted is remote. Finally, the Governmental Unit is aware that certain Scanning services could potentially damage software, applications, and/or data installed on its IT equipment. This is to be expected and may require the re-installation of the Governmental Unit's operating system, applications, programs, and data. The likelihood of potential damage from using Scanning services is remote.

The Governmental Unit UNDERSTANDS THE POTENTIAL LOSS OF DATA due to the scanning process in the detection of malware infections; data may get damaged, deleted, or at worst a data incident may occur. MNIT must inform the Governmental Unit of this possibility in using MNIT's tool. The Governmental Unit understands that MNIT will not accept liability for any loss of data as a result of the Governmental Unit's use or misuse of MNIT's tool. The Governmental Unit is responsible for backing up its own data.

The Governmental Unit UNDERSTANDS MNIT'S PRIVACY OBLIGATION, and that MNIT will not browse through the Governmental Unit data while assisting in the deployment of the Scanning tools or assessment of the results. However, as part of its incident response investigation, MNIT may be engaging in analysis of the data stored within the Governmental Unit's data environment that would require MNIT to review, examine, study, or separate the data. The Governmental Unit acknowledges its responsibility to protect any personal or private information. Additionally, MNIT may be required to report illegal content such as images or videos to law enforcement agencies, if discovered.

The Governmental Unit FULLY ACCEPTS AND ASSUMES ALL SUCH RISKS AND ALL RESPONSIBILITY for losses, costs, and damages the Governmental Unit incurs as a result of the Governmental Unit's participation and use, and the Governmental Unit's potential misuse of MNIT's tool.

The Governmental Unit HEREBY RELEASES AND DISCHARGES MNIT, the deployer of the scanning tools and the entity performing the security assessment, from all liability, claims, demands, losses, or damages that the Governmental Unit suffers which are caused or alleged to be caused in whole or in part by the Governmental Unit's use of MNIT's tool and the requested security assessment.

MY SIGNATURE BELOW CONFIRMS I HAVE READ, UNDERSTAND, AND AGREE TO BE BOUND BY THESE TERMS AND CONDITIONS

Chris Sutch

Name of Governmental Unit Representative

Signature of Governmental Unit Representative

Date

CROWDSTRIKE TERMS AND CONDITIONS

These CrowdStrike Terms and Conditions by and between CrowdStrike, Inc., a Delaware corporation, and any Affiliates performing hereunder (collectively, "**CrowdStrike**") with a principal place of business at 150 Mathilda Place, Suite 300, Sunnyvale, California 94086 and the State of Minnesota, Office of MN.IT Services, for itself and on behalf of Minnesota state agencies ("**Customer**"), with a place of business at 658 Cedar Street, St. Paul, MN 55155 are entered into as of the date signed by the last party (the "**Effective Date**").

These CrowdStrike Terms and Conditions (the "Agreement") are a master agreement that cover all CrowdStrike products and services but provisions regarding specific products or services apply only to the extent Customer has purchased, accessed or used such products or services. The Agreement supersedes any and all licensing or maintenance terms and conditions not agreed to in writing and signed by both parties, including any pre-installation or other "click-through" agreements. A State employee's decision to choose "accept" or an equivalent option associated with a "click-through" agreement or customer portal does not constitute the State's concurrence or acceptance of additional terms or conditions except for FedRamp Rules of Behavior agreements. Customer does not agree to any third party terms and conditions that are in conflict with the Agreement or applicable Minnesota law.

1. Definitions.

"**Affiliate**" means any entity that a party directly or indirectly controls (e.g., subsidiary) or is controlled by (e.g., parent) or with which it is under common control (e.g., sibling) or a Minnesota state entity whose information technology environment is managed in whole or in part by Customer.

"Agreement" means these CrowdStrike Terms and Conditions together with each Order.

"**API**" means an application program (or programming) interface.

"**CrowdStrike Competitor**" means a person or entity in the business of developing, distributing, or commercializing Internet security products or services substantially similar to or competitive with CrowdStrike's products or services.

"CrowdStrike Data" shall mean the data generated by the CrowdStrike Offerings, including but not limited to, correlative and/or contextual data, and/or detections. For the avoidance of doubt, CrowdStrike Data does not include Customer Data.

"**CrowdStrike Tool**" means any CrowdStrike proprietary software-as-a-service, software, hardware, or other tool that CrowdStrike uses in performing Professional Services, which may be specified in the applicable SOW. CrowdStrike Tools may include CrowdStrike's products.

"**Customer**" means as the context requires, in addition to the entity identified above, any Customer Affiliate that places an Order under these CrowdStrike Terms and Conditions, uses or accesses any Offering hereunder, or benefits from the Customer's use of an Offering.

"Customer Contractor" means any individual or entity (other than a CrowdStrike Competitor) that: (i) has access or use of a Product under this Agreement solely on behalf of and for Customer's Internal Use, (ii) has an agreement to provide Customer (or its Affiliates) services, and (iii) is subject to confidentiality obligations covering CrowdStrike's Confidential Information.

"**Customer Contractor Services**" means products, services or content developed or provided by Customer Contractors, including, but not limited to, third party applications complimentary to the Offerings, implementation services, managed services, training, technical support, or other consulting services related to, or in conjunction with, the Offerings.

"**Documentation**" means CrowdStrike's end-user technical documentation included in the applicable Offering.

"Endpoint" means any physical or virtual device, such as, a computer, server, laptop, desktop computer, mobile, cellular, container or virtual machine image.

"**Error**" means a reproducible failure of a Product to perform in substantial conformity with its applicable Documentation.

"**Internal Use**" means access or use solely for Customer's and subject to the Section entitled *Affiliates, Orders and Payment; Affiliates* and the Section entitled *Access and Use Rights*, its Affiliates', own internal information security purposes. By way of example and not limitation, Internal Use does not include access or use: (i) for the benefit of any person or entity other than Customer or its Affiliates, or (ii) in any event, for the development of any product or service. Internal Use is limited to access and use by Customer's and its Affiliates' employees and Customer or Affiliate Contractors (except as set forth in the Section entitled *Customer Contractors*), in either event, solely on Customer's behalf and for Customer's benefit.

"**Offerings**" means, collectively, any Products, Product-Related Services, or Professional Services.

"**Order**" means any purchase order or other ordering document (including any SOW) accepted by CrowdStrike or a reseller that identifies the following ordered by Customer: Offering, Offering quantity based on CrowdStrike's applicable license metrics (e.g., number of Endpoints, size of company (based on number of employees), number of file uploads, or number of queries), price and Subscription/Order Term.

"**Product**" means any of CrowdStrike's cloud-based software or other products ordered by Customer as set forth in the relevant Order, the available accompanying API's, the CrowdStrike Data, any Documentation and any Updates thereto that may be made available to Customer from time to time by CrowdStrike.

"**Product-Related Services**" means, collectively, (i) Falcon OverWatch, (ii) Falcon Complete Team, (iii) the technical support services for certain Products provided by CrowdStrike, (iv) training, and (v) any other CrowdStrike services provided or sold with Products. Product-Related Services do not include Professional Services.

"**Professional Services**" means any professional services performed by CrowdStrike for Customer pursuant to an SOW or other Order. Professional Services may include without limitation incident response, investigation and forensic services related to cyber-security adversaries, tabletop exercises, and next generation penetration tests related to cyber-security.

"**Services**" means, collectively, any Product-Related Services and any Professional Services.

"**Statement of Work**" or "**SOW**" means a mutually-agreed executed written document describing the Professional Services to be performed by CrowdStrike for Customer, deliverables, fees, and expenses related thereto.

"**Subscription/Order Term**" means the period of time set forth in the applicable Order during which: (i) Customer is authorized by CrowdStrike to access and use the Product or Product-Related Service, or (ii) Professional Services may be performed.

"**Updates**" means any correction, update, upgrade, patch, or other modification or addition made by CrowdStrike to any Product and provided to Customer by CrowdStrike from time to time on an as available basis.

2. Affiliates, Orders and Payment.

2.1 Affiliates. Any Affiliate purchasing hereunder, or using or accessing any Offering hereunder, or benefitting from the Customer's use of an Offering, will be bound by and comply with all terms and conditions of this Agreement. The Customer signing these CrowdStrike Terms and Conditions will remain responsible for Customer's Affiliates' acts and omissions unless Customer's Affiliate has entered into its own Terms and Conditions with CrowdStrike.

2.2 Orders. Only those transaction-specific terms stating the Offerings ordered, quantity, price, payment terms, Subscription/Order Term, and billing/provisioning contact information (and for the avoidance of doubt, specifically excluding any pre-printed terms on a Customer or reseller purchase order) will have any force or effect unless a particular Order is executed by both the Customer and an authorized signer of CrowdStrike and returned to Customer (or the applicable reseller). If any such Order is so executed and delivered, then only those specific terms on the face of such Order that expressly identify those portions of this Agreement that are to be superseded will prevail over any conflicting terms herein but only with respect to those Offerings ordered on such Order. Orders are

non-cancellable. Any Order through a reseller is subject to, and CrowdStrike's obligations and liabilities to Customer are governed by, this Agreement.

2.3 Payment and Taxes. Customer will pay the fees for Offerings to a reseller or CrowdStrike as set forth in the applicable Order. Unless otherwise expressly set forth on the Order, Customer will pay the fees and amounts stated on each Order within 30 days after receipt of the applicable invoice. Except as otherwise expressly provided in this Agreement, all fees and other amounts are non-refundable. Fees are exclusive of any applicable sales, use, value added, withholding, and other taxes, however designated. Customer shall pay all such taxes levied or imposed by reason of Customer's purchase of the Offerings and the transactions hereunder, except for taxes based on CrowdStrike's income or with respect to CrowdStrike's employment of its employees.

3. Access & Use Rights.

3.1 Evaluation. If CrowdStrike approves Customer's evaluation use of a CrowdStrike product ("**Evaluation Product**"), the terms herein applicable to Products also apply to evaluation access and use of such Evaluation Product, except for the following different or additional terms: (i) the duration of the evaluation is as mutually agreed upon by Customer and CrowdStrike, provided, that either CrowdStrike or Customer can terminate the evaluation at any time upon written (including email) notice to the other party; (ii) the Evaluation Product is provided "AS-IS" without warranty of any kind, and CrowdStrike disclaims all warranties, support obligations, and other liabilities and obligations for the Evaluation Product; and (iii) Customer's access and use is limited to Internal Use by Customer employees only. For avoidance of doubt, the limitations above do not apply to deployment of CrowdStrike product for proof of concept or proof of value purposes when Customer pays the appropriate pro-rated fees.

3.2 Access & Use Rights. Subject to the terms and conditions of this Agreement (including CrowdStrike's receipt of applicable fees), CrowdStrike grants Customer, under CrowdStrike's intellectual property rights in and to the applicable Product, a non-exclusive, non-transferable (except as expressly provided in the Section entitled *Assignment*), non-sublicensable license to access and use the Products in accordance with any applicable Documentation solely for Customer's Internal Use during the applicable Subscription/Order Term. Customer's access and use is limited to the quantity in the applicable Order. Furthermore, the following additional terms and conditions apply to specific Products (or components thereof):

(a) Products with Software Components. If Customer purchases a subscription to a Product with a downloadable object-code component ("**Software Component**"), Customer may, during the Subscription/Order Term install and run multiple copies of the Software Components solely for Customer's and Customer's Affiliates' Internal Use up to the maximum quantity in the applicable Order.

(b) CrowdStrike Tools. If CrowdStrike provides CrowdStrike Tools to Customer pursuant to performing Professional Services, the license set forth in the Section entitled *Access & Use Rights* applies to such CrowdStrike Tools as used solely for Customer's Internal Use during the period of time set forth in the applicable Order, or if none is specified, for the period authorized by CrowdStrike. Not all Professional Services engagements will involve the use of CrowdStrike Tools.

3.3 Restrictions. The access and use rights set forth in the Section entitled *Access & Use Rights* do not include any rights to, and Customer will not, with respect to any Offering (or any portion thereof): (i) knowingly allow or authorize a CrowdStrike Competitor to use or view the Offering or Documentation, or to provide management, hosting, or support for an Offering; (ii) alter, publicly display, translate, create derivative works of or otherwise modify an Offering; (iii) sublicense, distribute or otherwise transfer an Offering to any third party (except as expressly provided in the Section entitled *Assignment*); (iv) allow third parties to access or use an Offering (except for Customer Contractors as expressly permitted herein); (v) create public Internet "links" to an Offering or "frame" or "mirror" any Offering content on any other server or wireless or Internet-based device; (vi) reverse engineer, decompile, disassemble or otherwise attempt to derive the source code (if any) for an Offering (except to the extent that such prohibition is expressly precluded by applicable law), circumvent its functions, or attempt to gain unauthorized access to an Offering or its related systems or networks; (vii) use an Offering to circumvent the security of another party's network/information, develop malware, unauthorized surreptitious surveillance, data modification, data exfiltration, data ransom or data destruction; (viii) remove or alter any notice of proprietary right appearing on an Offering; (ix) conduct any stress tests, competitive benchmarking or analysis on, or publish any performance data of, an Offering (provided, that this does not prevent Customer from comparing the Products to other products for

Customer's Internal Use); (x) use any feature of CrowdStrike APIs for any purpose other than in the performance of, and in accordance with, this Agreement; or (xi) cause, encourage or assist any third party to do any of the foregoing. Customer agrees to use an Offering in accordance with laws, rules and regulations directly applicable to Customer and acknowledges that Customer is solely responsible for determining whether a particular use of an Offering is compliant with such laws.

3.4 Installation and User Accounts. CrowdStrike is not responsible for installing Products unless Customer purchases installation services from CrowdStrike. For those Products requiring user accounts, only the single individual user assigned to a user account may access or use the Product. Customer is liable and responsible for all actions and omissions occurring under Customer's and Customer Contractor's user accounts for Offerings. Customer shall notify CrowdStrike if Customer learns of any unauthorized access or use of Customer's user accounts or passwords for an Offering.

3.5 Malware Samples. If CrowdStrike makes malware samples available to Customer in connection with an evaluation or use of the Product ("**Malware Samples**"), Customer acknowledges and agrees that: (i) Customer's access to and use of Malware Samples is at Customer's own risk, and (ii) Customer should not download or access any Malware Samples on or through its own production systems and networks and that doing so can infect and damage Customer's systems, networks, and data. Customer shall use the Malware Samples solely for Internal Use and not for any malicious or unlawful purpose. CrowdStrike will not be liable for any loss or damage caused by any Malware Sample that may infect Customer's computer equipment, computer programs, data, or other proprietary material due to Customer's access to or use of the Malware Samples.

3.6 Third Party Software. CrowdStrike uses certain third party software in its Products, including what is commonly referred to as open source software. Under some of these third party licenses, CrowdStrike is required to provide Customer with notice of the license terms and attribution to the third party. See the licensing terms and attributions for such third party software that CrowdStrike uses at: https://falcon.crowdstrike.com/opensource.

3.7 Ownership & Feedback. Products, Product-Related Services and the CrowdStrike Tools are made available for use or licensed, not sold. CrowdStrike owns and retains all right, title and interest (including all intellectual property rights) in and to the Products, Product-Related Services and the CrowdStrike Tools. Any feedback or suggestions that Customer provides to CrowdStrike regarding its Offerings and CrowdStrike Tools (e.g., bug fixes and features requests) is non-confidential and may be used by CrowdStrike for any purpose without acknowledgement or compensation; provided, Customer will not be identified publicly as the source of the feedback or suggestion.

4. Customer Contractors.

4.1 Authorization. Customer authorizes CrowdStrike to give Customer Contractors the rights and privileges to the Offerings necessary to enable and provide for Customer's use and receipt of the Customer Contractor Services. If at any time Customer revokes this authorization, to the extent the Offerings provide for Customer to limit the Customer Contractor's access and use of the Offerings, then Customer is responsible for taking the actions necessary to revoke such access and use. In the event Customer requires CrowdStrike assistance with such revocation or limitation, Customer must contact CrowdStrike Support with written notice of such revocation or limitation at support@crowdstrike.com and CrowdStrike will disable the Customer Contractor's access to Customer's Offerings within a reasonable period of time following receipt of such notice but in any event within 72 hours of receipt of such notice.

4.2 Disclaimer. Customer Contractors are subject to the terms and conditions in the Agreement while they are using the Offerings on behalf of Customer and Customer remains responsible for their acts and omissions during such time. Any breach by a Customer Contractor of this Agreement is a breach by Customer. CrowdStrike may make available Customer Contractor Services to Customer, for example, through an online directory, catalog, store, or marketplace. Customer Contractor Services are not required for use of the Offerings. Offerings may contain features, including API's, designed to interface with or provide data to Customer Contractor Services. CrowdStrike is not responsible or liable for any loss, costs or damages arising out of Customer Contractor's actions or inactions in any manner, including but not limited to, for any disclosure, transfer, modification or deletion of Customer Data (defined in Exhibit A). Whether or not a Customer Contractor is designated by CrowdStrike as, or otherwise claims to be "certified," "authorized," or similarly labeled, CrowdStrike does not: (i) control, monitor, maintain or provide support for, Customer Contractor Services, (ii) disclaims all warranties of any kind, indemnities, obligations, and

other liabilities in connection with the Customer Contractor Services, and any Customer Contractor interface or integration with the Offerings, and (iii) cannot guarantee the continued availability of Customer Contractor Services and related features. If Customer Contractor Services and related features are no longer available for any reason, CrowdStrike is not obligated to provide any refund, credit, or other compensation for, or related to, the Offerings.

4.3 Restrictions on Customer Contractors. Customer shall not give or allow Customer Contractors access to, or use of, intelligence reports provided by, or made accessible in, the Products. For the avoidance of doubt, nothing herein prevents Customer from using intelligence API's in Customer Contractor Services for Customer's Internal Use.

5. Professional Services.

Reserved.

6. Data Security and Privacy. See Exhibit A.

7. Confidentiality.

7.1 Definitions. In connection with this Agreement, each party ("**Recipient**") may receive Confidential Information of the other party ("**Discloser**") or third parties to whom Discloser has a duty of confidentiality. "**Confidential Information**" means non-public information in any form that is in the Recipient's possession regardless of the method of acquisition that the Discloser designates as confidential to Recipient, should be reasonably known by the Recipient to be Confidential Information due to the nature of the information disclosed and/or the circumstances surrounding the disclosure, or is not publicly accessible under the Minnesota Government Data Practices Act (Minnesota Statutes chapter 13). Confidential Information shall not include information that is: (i) in or becomes part of the public domain (other than by disclosure by Recipient in violation of this Agreement); (ii) previously known to Recipient without an obligation of confidentiality and demonstrable by the Recipient; (iii) independently developed by Recipient without use of Discloser's Confidential Information; (iv) rightfully obtained by Recipient from third parties without an obligation of confidentiality; or (v) determined to be publicly accessible under the Minnesota Government Data Practices Act (Minnesota Statutes chapter 13). Customer agrees to provide CrowdStrike reasonable notice prior to disclosing any CrowdStrike Confidential Information in response to a valid request made pursuant to the Minnesota Government Data Practices Act to allow CrowdStrike to seek injunctive relief or such other relief as may be appropriate.

7.2 Restrictions on Use. Except as allowed in Section 7.3 (*Exceptions*), Recipient shall hold Discloser's Confidential Information in strict confidence and shall not disclose any such Confidential Information to any third party, other than to its employees, and contractors, including without limitation, counsel, accountants, and financial advisors (collectively, "Representatives"), its Affiliates and their Representatives, subject to the other terms of this Agreement, and in each case who need to know such information and who are bound by restrictions regarding disclosure and use of such information comparable to and no less restrictive than those set forth herein. Recipient shall not use Discloser's Confidential Information for any purpose other than as set forth in this Agreement. Recipient shall take the same degree of care that it uses to protect its own confidential information of a similar nature and importance (but in no event less than reasonable care) to protect the confidentiality and avoid the unauthorized use, disclosure, publication, or dissemination of the Discloser's Confidential Information. Within 72 hours of Recipient becoming aware of the unauthorized use, disclosure, publication, or dissemination of the Discloser's Confidential Information while in Recipient's control, Recipient shall provide Discloser with notice thereof.

7.3 Exceptions. Recipient may disclose Discloser's Confidential Information: (i) to the extent required by applicable law or regulation; (ii) pursuant to a subpoena or order of a court or regulatory, self-regulatory, or legislative body of competent jurisdiction; (iii) in connection with any regulatory report, audit, or inquiry; or (iv) where requested by a regulator with jurisdiction over Recipient. In the event of such a requirement or request, Recipient shall, to the extent legally permitted: (a) give Discloser prompt written notice of such requirement or request prior to such disclosure; and (b) at Discloser's cost, a reasonable opportunity to review and comment upon the disclosure and request confidential treatment or a protective order pertaining thereto prior to Recipient making such disclosure.

7.4 Destruction. Upon Discloser's written request, Recipient shall use commercially reasonable efforts to destroy the Confidential Information and any copies or extracts thereof. However, Recipient, its Affiliates and their Representatives may retain any Confidential Information that: (i) they are required to keep for compliance purposes under a document retention policy or as required by applicable law, professional standards, a court, or regulatory

agency; or (ii) have been created electronically pursuant to automatic or ordinary course archiving, back-up, security, or disaster recovery systems or procedures; provided, however, that any such retained information shall remain subject to this Agreement. Upon Discloser's request, Recipient will provide Discloser with written confirmation of destruction in compliance with this provision.

7.5 Equitable Relief. Each party acknowledges that a breach of this Section 7 (*Confidentiality*) shall cause the other party irreparable injury and damage. Therefore, each party agrees that those breaches may be stopped through injunctive proceedings in addition to any other rights and remedies which may be available to the injured party at law or in equity without the posting of a bond.

8. Warranties & Disclaimer.

8.1 No Warranty for Pre-Production Versions. Any pre-production feature or version of an Offering provided to Customer is *experimental* and provided "AS IS" without warranty of any kind and will not create any obligation for CrowdStrike to continue to develop, productize, support, repair, offer for sale, or in any other way continue to provide or develop any such feature or Offering. Customer agrees that its purchase is not contingent on the delivery of any future functionality or features, or dependent on any oral or written statements made by CrowdStrike regarding future functionality or features.

8.2 Product Warranty. If Customer has purchased a Product, CrowdStrike warrants to Customer during the applicable Subscription/Order Term that: (i) the Product will operate without Error; and (ii) CrowdStrike has used industry standard techniques to prevent the Products at the time of delivery from injecting malicious software viruses into Customer's Endpoints where the Products are installed. Customer must notify CrowdStrike of any warranty claim during the Subscription/Order Term. Customer's sole and exclusive remedy and the entire liability of CrowdStrike for its breach of this warranty will be for CrowdStrike, at its own expense to do at least one of the following: (a) use commercially reasonable efforts to provide a work-around or correct such Error; or (b) terminate Customer's license to access and use the applicable non-conforming Product and refund the prepaid fee prorated for the unused period of the Subscription/Order Term. CrowdStrike shall have no obligation regarding Errors reported after the applicable Subscription/Order Term.

8.3 Services Warranty. CrowdStrike warrants to Customer that it will perform all Services in a professional and workmanlike manner consistent with generally accepted industry standards. Customer must notify CrowdStrike of any warranty claim for Services during the period the Services are being performed or within 30 days after the conclusion of the Services. Customer's sole and exclusive remedy and the entire liability of CrowdStrike for its breach of this warranty will be for CrowdStrike, at its option and expense, to (a) use commercially reasonable efforts to re-perform the non-conforming Services, or (b) refund the portion of the fees paid attributable to the non-conforming Services.

8.4 Exclusions. The express warranties do not apply if the applicable Product or Service: (i) has been modified, except by CrowdStrike, (ii) has not been installed, used, or maintained in accordance with this Agreement or Documentation, or (iii) is non-conforming due to a failure to use an applicable Update. If any part of a Product or Service references websites, hypertext links, network addresses, or other third party locations, information, or activities, it is provided as a convenience only.

8.5 No Guarantee. CUSTOMER ACKNOWLEDGES, UNDERSTANDS, AND AGREES THAT CROWDSTRIKE DOES NOT GUARANTEE OR WARRANT THAT IT WILL FIND, LOCATE, OR DISCOVER ALL OF CUSTOMER'S OR ITS AFFILIATES' SYSTEM THREATS, VULNERABILITIES, MALWARE, AND MALICIOUS SOFTWARE, AND CUSTOMER AND ITS AFFILIATES WILL NOT HOLD CROWDSTRIKE RESPONSIBLE THEREFOR.

8.6 Disclaimer. EXCEPT FOR THE EXPRESS WARRANTIES IN THIS SECTION 8, CROWDSTRIKE AND ITS AFFILIATES DISCLAIM ALL OTHER WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE. TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, CROWDSTRIKE AND ITS AFFILIATES AND SUPPLIERS SPECIFICALLY DISCLAIM ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGMENT WITH RESPECT TO THE OFFERINGS AND CROWDSTRIKE TOOLS. THERE IS NO WARRANTY THAT THE OFFERINGS OR CROWDSTRIKE TOOLS WILL BE ERROR FREE, OR THAT THEY WILL OPERATE WITHOUT INTERRUPTION OR WILL FULFILL ANY OF CUSTOMER'S PARTICULAR PURPOSES OR NEEDS. THE OFFERINGS AND CROWDSTRIKE TOOLS ARE NOT FAULT-TOLERANT AND ARE NOT DESIGNED OR INTENDED FOR USE IN

ANY HAZARDOUS ENVIRONMENT REQUIRING FAIL-SAFE PERFORMANCE OR OPERATION. NEITHER THE OFFERINGS NOR CROWDSTRIKE TOOLS ARE FOR USE IN THE OPERATION OF AIRCRAFT NAVIGATION, NUCLEAR FACILITIES, COMMUNICATION SYSTEMS, WEAPONS SYSTEMS, DIRECT OR INDIRECT LIFE-SUPPORT SYSTEMS, AIR TRAFFIC CONTROL, OR ANY APPLICATION OR INSTALLATION WHERE FAILURE COULD RESULT IN DEATH, SEVERE PHYSICAL INJURY, OR PROPERTY DAMAGE. Customer agrees that it is Customer's responsibility to ensure safe use of an Offering and the CrowdStrike Tools in such applications and installations. CROWDSTRIKE DOES NOT WARRANT ANY THIRD PARTY PRODUCTS OR SERVICES.

9. Indemnification.

9.1 CrowdStrike's Obligation. CrowdStrike shall at its cost and expense: (i) defend and/or settle any claim brought against Customer by an unaffiliated third party alleging that an Offering infringes or violates that third party's intellectual property rights, and (ii) pay and indemnify any settlement of such claim or any damages awarded to such third party by a court of competent jurisdiction as a result of such claim; provided, that Customer: (a) gives CrowdStrike prompt written notice of such claim; (b) permits CrowdStrike to solely control and direct the defense or settlement of such claim (however, CrowdStrike will not settle any claim in a manner that requires Customer to admit liability without Customer's prior written consent); and (c) provides CrowdStrike all reasonable assistance in connection with the defense or settlement of such claim, at CrowdStrike's cost and expense. In addition, Customer may, at Customer's own expense, participate in defense of any claim. To the extent required by applicable law, any defense under this section shall be subject to the initial consent and approval of the Minnesota Attorney General.

9.2 Remedies. If a claim covered under this Section occurs or in CrowdStrike's opinion is reasonably likely to occur, CrowdStrike may at its expense and sole discretion (and if Customer's access and use of an Offering is enjoined, CrowdStrike will, at its expense): (i) procure the right to allow Customer to continue using the applicable Offering; (ii) modify or replace the applicable Offering to become non-infringing; or (iii) if neither (i) nor (ii) is commercially practicable, terminate Customer's license or access to the affected portion of applicable Offering and refund a portion of the pre-paid, unused fees paid by Customer corresponding to the unused period of the Subscription/Order Term.

9.3 Exclusions. CrowdStrike shall have no obligations under this Section if the claim is based upon or arises out of: (i) any modification to the applicable Offering not made by CrowdStrike; (ii) any combination or use of the applicable Offering with or in any third party software, hardware, process, firmware, or data, to the extent that such claim is based on such combination or use; (iii) Customer's continued use of the allegedly infringing Offering after being notified of the infringement claim or after being provided a modified version of the Offering by CrowdStrike at no additional cost that is intended to address such alleged infringement; (iv) Customer's failure to use the Offering in accordance with the applicable Documentation; and/or (v) Customer's use of the Offering outside the scope of the rights granted under this Agreement.

9.4 Exclusive Remedy. THE REMEDIES SPECIFIED IN THIS SECTION CONSTITUTE CUSTOMER'S SOLE AND EXCLUSIVE REMEDIES, AND CROWDSTRIKE'S ENTIRE LIABILITY, WITH RESPECT TO ANY INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

10. Limitation of Liability.

10.1 TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, EXCEPT FOR LIABILITY FOR ANY AMOUNTS PAID OR PAYABLE TO THIRD PARTIES UNDER SECTION 9 (*INDEMNIFICATION*), CUSTOMER'S PAYMENT OBLIGATIONS, AND/OR ANY INFRINGEMENT OR MISAPPROPRIATION BY ONE PARTY OF THE OTHER PARTY'S INTELLECTUAL PROPERTY RIGHTS, NEITHER PARTY SHALL BE LIABLE TO THE OTHER PARTY IN CONNECTION WITH THIS AGREEMENT OR THE SUBJECT MATTER HEREOF (UNDER ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STATUTE, TORT OR OTHERWISE) FOR ANY LOST PROFITS, REVENUE, OR SAVINGS, LOST BUSINESS OPPORTUNITIES, LOST DATA, OR SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR PUNITIVE DAMAGES, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSSES OR SUCH DAMAGES OR LOSSES WERE REASONABLY FORESEEABLE; OR (B) AN AMOUNT THAT EXCEEDS THE TOTAL FEES PAID OR PAYABLE TO CROWDSTRIKE FOR THE RELEVANT OFFERING DURING THAT OFFERING'S SUBSCRIPTION/ORDER TERM PROVIDED, HOWEVER, THAT IN THE EVENT OF A CLAIM RESULTING FROM A PARTY'S BREACH OF SECTION 7 (CONFIDENTIALITY) OR BREACH OF EXHIBIT A WHICH RESULTS IN THE COMPROMISE OF CUSTOMER DATA OR PERSONAL DATA, THE BREACHING PARTY'S LIABILITY SHALL NOT EXCEED AN

AMOUNT IN EXCESS OF THREE TIMES (3X) THE TOTAL FEES PAID OR PAYABLE TO CROWDSTRIKE FOR THE RELEVANT OFFERING DURING THAT OFFERING'S SUBSCRIPTION/ORDER TERM. THESE LIMITATIONS WILL APPLY NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY REMEDY SPECIFIED IN THIS AGREEMENT. MULTIPLE CLAIMS SHALL NOT EXPAND THE LIMITATIONS SPECIFIED IN THIS SECTION 10. THIS PROVISION DOES NOT LIMIT EITHER PARTY'S LIABILITY FOR: DEATH OR BODILY INJURY CAUSED BY THEIR NEGLIGENCE; ACTS OF FRAUD OR WILLFUL MISCONDUCT UNDER THE AGREEMENT; OR ANY LIABILITY THAT MAY NOT BE EXCLUDED OR LIMITED BY APPLICABLE LAW.

11. Compliance with Laws. Each party agrees to comply with all U.S. federal, state, local and non-U.S. laws directly applicable to such party in the performance of this Agreement, including but not limited to, applicable export and import, anti-corruption and employment laws. Customer acknowledges and agrees the Offerings shall not be used, transferred, or otherwise exported or re-exported to regions that the United States and/or the European Union maintains an embargo or comprehensive sanctions (collectively, "Embargoed Countries"), or to or by a national or resident thereof, or any person or entity subject to individual prohibitions (e.g., parties listed on the U.S. Department of Treasury's List of Specially Designated Nationals or the U.S. Department of Commerce's Table of Denial Orders) (collectively, "Designated Nationals"), without first obtaining all required authorizations from the U.S. government and any other applicable government. Customer represents and warrants that Customer is not located in, or is under the control of, or a national or resident of, an Embargoed Country or Designated National. CrowdStrike represents and warrants that CrowdStrike is not located in, or is under the control of, or a national or resident of, an Embargoed Country or Designated National.

12. U.S. Government End Users.

12.1 Commercial Items. The following applies to all acquisitions by or for the U.S. government or by any U.S Government prime contractor or subcontractor at any tier ("Government Users") under any U.S. Government contract, grant, other transaction, or other funding agreement. The Products, CrowdStrike Tools, and Documentation are "commercial items," as that term is defined in Federal Acquisition Regulation ("FAR") (48 C.F.R.) 2.101, consisting of "commercial computer software" and "commercial computer software documentation," as such terms are used in FAR 12.211 and 12.212. In addition, Department of Defense FAR Supplement ("DFARS") 252.227-7015 (Technical Data – Commercial Items) applies to technical data acquired by Department of Defense agencies. Consistent with FAR 12.211 and 12.212 and DFARS (48 C.F.R.) 227.7202-1 through 227.7202-4, the Products, CrowdStrike Tools, and Documentation are being licensed to Government Users pursuant to the terms of this license(s) customarily provided to the public as forth in this Agreement, unless such terms are inconsistent with United States federal law ("Federal Law").

12.2 Disputes with the U.S. Government. If this Agreement fails to meet the Government's needs or is inconsistent in any way with Federal Law and the parties cannot reach a mutual agreement on terms for this Agreement, the Government agrees to terminate its use of the Offerings. In the event of any disputes with the U.S. Government in connection with this Agreement, Section 14.3 of this Agreement shall not apply. Instead the rights and duties of the parties arising from this Agreement, shall be governed by, construed, and enforced in accordance with Federal Procurement Law and any such disputes shall be resolved pursuant to the Contract Disputes Act of 1978, as amended (41 U.S.C. 7101-7109), as implemented by the Disputes Clause, FAR 52.233-1.

12.3 Precedence. This U.S. Government rights in this Section are in lieu of, and supersedes, any other FAR, DFARS, or other clause, provision, or supplemental regulation that addresses Government rights in the Offerings, computer software or technical data under this Agreement.

13. Suspension and Termination. This Agreement shall remain effective until termination in accordance with this Section or as otherwise specified herein. CrowdStrike may immediately suspend Customer's access to, or use of, the Offerings if: (i) CrowdStrike believes that there is a significant threat to the security, integrity, functionality, or availability of the Offerings or any content, data, or applications in the Offerings; (ii) Customer or Customer users are in breach of Section 3.4 (*Restrictions*); or (iii) Customer fails to pay CrowdStrike when undisputed fees are due; provided, however, CrowdStrike will use commercially reasonable efforts under the circumstances to provide Customer with notice and, if applicable, an opportunity to remedy such violation prior to any such suspension. Either party may terminate this Agreement upon 30 days' written notice of a material breach by the other party, unless the breach is cured within the 30-day notice period. Prior to termination and subject to the terms of this Agreement, Customer shall have the right to access and download Customer Data available per the Customer's purchased Products and data retention period in a manner and in a format supported by the Products. Upon termination of this

Agreement for any reason: (a) all Customer's access and use rights granted in this Agreement will terminate; (b) Customer must promptly cease all use of Offerings and de-install all Software Components installed on Customer's Endpoints; and (c) Customer Data will be deleted in accordance with the data retention period purchased by Customer and Section 7.4 *Confidentiality; Destruction*). Sections 1, 3.4, 7, 10, 12, 13, and 14 and all liabilities that accrue prior to termination shall survive expiration or termination of this Agreement for any reason.

13.1 Termination by Customer. Customer may terminate this Agreement at any time for convenience upon thirty (30) calendar days written notice; provided, however, that Customer (a) shall not be entitled to any refund of prepaid fees, (b) shall pay all fees for any Offerings ordered prior to the effective date of termination, and (c) shall pay all fees and expenses that have accrued prior to the effective date of termination. Customer may terminate this Agreement for cause in the event of material breach of the Agreement by CrowdStrike, in which case Customer shall be entitled to a pro-rata refund of fees paid and shall be relieved of all future payment obligations. Upon termination by Customer for any reason Customer shall have the right to access and download Customer Data available per the Customer's purchased Products and data retention period in a manner and in a format supported by the Products.

13.2 Funding Out Clause. Customer may immediately cancel this Agreement if it does not obtain funding from the Minnesota Legislature, or other funding source; or if funding cannot be continued at a level sufficient to allow for the payment of the Offerings covered here. Notwithstanding the foregoing, (1) with each Order, Customer must have provided a purchase order; and (2) Customer's issuance of such purchase order shall signify to CrowdStrike that all funds for the Order, which funds are or will become, pursuant to such Order, due and payable in the then current fiscal year, have been fully appropriated and are available and no longer subject to any appropriations contingency. Cancellation must be by written or facsimile transmission notice to CrowdStrike. Customer will not be assessed any penalty if this Agreement is cancelled because of a decision of the Minnesota Legislature, or other funding source, not to appropriate funds. Customer must provide CrowdStrike notice of the lack of funding within a reasonable time of the Customer's receiving that notice.

14. General.

14.1 Entire Agreement. This Agreement constitutes the entire agreement between Customer and CrowdStrike concerning the subject matter of this Agreement and it supersedes all prior and simultaneous proposals, agreements, understandings, or other communications between the parties, oral or written, regarding such subject matter. Notwithstanding the foregoing, if you have a CrowdStrike *Limited Warranty Agreement for Falcon Complete* (or a preceding or successor named product) fully executed with CrowdStrike, the warranty provided therein stands alone and is not superseded by this Agreement. It is expressly agreed that the terms of this Agreement shall supersede any terms in any procurement Internet portal or other similar non-CrowdStrike document and no such terms included in any such portal or other non-CrowdStrike document shall apply to the Offerings ordered. Any Order through a reseller is subject to, and CrowdStrike's obligations and liabilities to Customer are governed by, this Agreement. CrowdStrike is not obligated under any reseller's agreement with you unless an officer of CrowdStrike executes the agreement. This Agreement shall not be construed for or against any party to this Agreement because that party or that party's legal representative drafted any of its provisions.

14.2 Assignment. Neither party may assign this Agreement without the prior written consent of the other party, except to an Affiliate in connection with a corporate reorganization or in connection with a merger, acquisition, or sale of all or substantially all of its business and/or assets. Any assignment in violation of this Section shall be void. Subject to the foregoing, all rights and obligations of the parties under this Agreement shall be binding upon and inure to the benefit of and be enforceable by and against the successors and permitted assigns.

14.3 Governing Law; Venue. This Agreement, and the rights and duties of the parties arising from this Agreement, shall be governed by, construed, and enforced in accordance with the laws of the State of Minnesota, excluding its conflicts-of-law principles. The sole and exclusive jurisdiction and venue for actions arising under this Agreement shall be state and federal courts in Ramsey County, Minnesota, and the parties agree to service of process in accordance with the rules of such courts. The Uniform Computer Information Transactions Act and the United Nations Convention on the International Sale of Goods shall not apply. Notwithstanding the foregoing, each party reserves the right to file a suit or action in any court of competent jurisdiction as such party deems necessary to protect its intellectual property rights and, in CrowdStrike's case, to recoup any payments due.

14.4 Independent Contractors; No Third Party Rights. The parties are independent contractors. This Agreement shall not establish any relationship of partnership, joint venture, employment, franchise, or agency between the parties. No provision in this Agreement is intended or shall create any rights with respect to the subject matter of this Agreement in any third party.

14.5 Waiver, Severability & Amendments. The failure of either party to enforce any provision of this Agreement shall not constitute a waiver of any other provision or any subsequent breach. If any provision of this Agreement is held to be illegal, invalid, or unenforceable, the provision will be enforced to the maximum extent permissible so as to affect the intent of the parties, and the remaining provisions of this Agreement will remain in full force and effect. This Agreement may only be amended, or any term or condition set forth herein waived, by written consent of both parties.

14.6 Force Majeure. Neither party shall be liable for, nor shall either party be considered in breach of this Agreement due to, any failure to perform its obligations under this Agreement (other than its payment obligations) as a result of a cause beyond its control, including but not limited to, act of God or a public enemy, act of any military, civil or regulatory authority, change in any law or regulation, fire, flood, earthquake, storm or other like event, disruption or outage of communications (including an upstream server block and Internet or other networked environment disruption or outage), power or other utility, labor problem, or any other cause, whether similar or dissimilar to any of the foregoing, which could not have been prevented with reasonable care. The party experiencing a force majeure event, shall use commercially reasonable efforts to provide notice of such to the other party.

14.7 Notices. All legal notices will be given in writing to the addresses in the first introductory paragraph of this Agreement and will be effective: (i) when personally delivered, (ii) on the reported delivery date if sent by a recognized international or overnight courier, or (iii) five business days after being sent by registered or certified mail (or ten days for international mail). For clarity, Orders, POs, confirmations, invoices, and other documents relating to order processing and payment are not legal notices and may be delivered electronically in accordance with each party's standard ordering procedures.

14.8 Signatures. This Agreement and any Orders may be executed in two counterparts, each of which will be considered an original but all of which together will constitute one agreement. Any signature delivered by electronic means shall be treated for all purposes as an original.

14.9 IT Accessibility. CrowdStrike acknowledges and is fully aware of the accessibility requirements of Minnesota Statutes section 16E.03 and the State of Minnesota Accessibility Standards – available online at http://mn.gov/mnit/images/Stnd_State_Accessibility.pdf or http://mn.gov/mnit/ – that incorporate both Section 508 of the Rehabilitation Act and Web Content Accessibility Guidelines 2.0 level 'AA'. The Standards apply to web sites, software applications, electronic reports and output documentation, training delivered in electronic formats (including, but not limited to, documents, videos, and webinars), among others.

The extent to which an Offering is, at the time of delivery, capable of providing comparable access to individuals with disabilities consistent with the applicable provisions of Section 508 of the Rehabilitation Act of 1973, in effect as of the Effective Date, is indicated by the comments and exceptions (if any) specified on the applicable Voluntary Product Accessibility Template (VPAT), provided that such Offering is used in accordance with the applicable Documentation and that any assistive technologies and any other products used with the Offering properly interoperate with such Offering. In the event that no VPAT is available for a particular Offering, the outcome may be that an Offering is still being evaluated for accessibility, may be scheduled to meet accessibility standards in a future release, or may not be scheduled to meet accessibility standards at all.

Upon Customer's request and pursuant to Section 3.1 hereof, CrowdStrike will allow Customer sufficient access to each Product prior to initial purchase for Customer evaluation of such Product by testing in Customer's production or non-production environment and review of the then-current VPAT and any additional information provided by CrowdStrike. CrowdStrike acknowledges that given Customer's statutory obligations to provide accessible IT solutions to users, nonconformance with the above referenced standards may limit its ability to purchase an Offering or expand its deployment by purchasing additional quantities of an Offering. If an Offering does not provide the comparable access described above and in the corresponding VPAT, Customer's sole and exclusive remedy and the entire liability of CrowdStrike for such failure will be for CrowdStrike, at its own expense to do at least one of the following: (a) use commercially reasonable efforts to rectify the deficiency; or (b) terminate Customer's license to

access and use the applicable non-conforming Offering and refund the prepaid fee prorated for the unused period of the Subscription/Order Term.

CROWDSTRIKE, INC.

DocuSigned by:
By: Mike Forman
B5DD7CD22354453...

Name: Mike Forman

Title: VP/Controller

Date: 1/25/2021

DS
MS

State of Minnesota, Office of MN.IT Services:

DocuSigned by:
By: Tracy Gerasch
58BF08075AF6441...

Name: Tracy Gerasch

Title: Procurement Director

Date: 1/28/2021

Exhibit A: Data Security and Privacy Schedule

1. **Definitions**
   a. **"CrowdStrike Systems"** means those computer systems hosting the 'Falcon EPP Platform'.
   b. **"Customer Data"** means the data generated by the Customer's Endpoint and collected by: (i) the Products, and/or (ii) the CrowdStrike Tools, and in either case, sent to the CrowdStrike Systems, which may include government data" in Minnesota Statutes section 13.02, subdivision 7 and "not public" customer data has the meaning in Minnesota Statutes section 13.02, subdivision 8a. Customer Data is considered Customer's Confidential Information (defined in Section 7 *Confidentiality*) and subject to the exclusions, exceptions and obligations set forth therein and this Exhibit A *Data Security and Privacy Schedule*.
   c. **"Execution Profile/Metric Data"** means any machine-generated data, such as metadata derived from tasks, file execution, commands, resources, network telemetry, executable binary files, macros, scripts, and processes, that: (i) Customer provides to CrowdStrike in connection with this Agreement or (ii) is collected or discovered during the course of CrowdStrike providing Offerings, excluding any such information or data that identifies Customer or to the extent it includes Personal Data.
   d. **"Personal Data"** means information provided by Customer to CrowdStrike or collected by CrowdStrike from Customer used to distinguish or trace a natural person's identity, either alone or when combined with other personal or identifying information that is linked or linkable by CrowdStrike to a specific natural person. Personal Data also includes such other information about a specific natural person to the extent that the data protection laws applicable in the jurisdictions in which such person resides define such information as Personal Data.
   e. **"Privacy and Security Laws"** means U.S. federal, state and local and non-U.S. laws, including those of the European Union, that regulate the privacy or security of Personal Data and that are directly applicable to CrowdStrike.
   f. "**Privacy Incident**" means violation of the Minnesota Government Data Practices Act (Minnesota Statutes chapter 13); violation of federal data disclosure or privacy requirements in federal laws, rules and regulations; and/or breach of a contractual obligation to protect Customer Data that results in the compromise of such Customer Data. This includes, unauthorized: access to, viewing of, obtaining of, acquisition of, use of, disclosure of, damage to, loss of, modification of, alteration to or destruction of Customer Data protected by such state or federal laws or by contract. Notwithstanding the foregoing, this shall not prevent CrowdStrike from performing its duties as provided for under this Agreement.
   g. **"Security Breach"** means unauthorized access to, or unauthorized acquisition of: (i) Customer Data, or (ii) Personal Data, stored on CrowdStrike Systems that results in the compromise of such Customer Data and/or Personal Data.
   h. **"Security Incident"** means any actual or successful: unauthorized access to, viewing of, obtaining of, acquisition of, use of, disclosure of, modification of, alteration to, loss of, damage to or destruction of Customer Data that results in the compromise of such Customer Data and/or Personal Data.
   i. **"Threat Actor Data"** means any malware, spyware, virus, worm, Trojan horse, or other potentially malicious or harmful code or files, URLs, DNS data, network telemetry, commands, processes or techniques, metadata, or other information or data, in each case that is potentially related to unauthorized third parties associated therewith and that: (i) Customer provides to CrowdStrike in connection with this Agreement, or (ii) is collected or discovered during the course of CrowdStrike providing Offerings, excluding any such information or data that identifies Customer or to the extent that it includes Personal Data.

2. **Falcon Platform**
   The 'Falcon EPP Platform' uses a crowd-sourced environment, for the benefit of all customers, to help customers protect themselves against suspicious and potentially destructive activities. CrowdStrike's Products are designed to detect, prevent, respond to, and identify intrusions by collecting and analyzing data, including machine event data, executed scripts, code, system files, log files, dll files, login data, binary files, tasks, resource information, commands, protocol identifiers, URLs, network data, and/or other executable code and metadata. Customer, rather than CrowdStrike, determines which types of data, whether Personal Data or not, exist on its systems. Accordingly, Customer's endpoint environment is unique in configurations and naming conventions and the machine event data could potentially include Personal Data. CrowdStrike uses the data to: (i) analyze, characterize, attribute, warn of, and/or respond to threats against Customer and other customer, (ii) analyze trends and performance, (iii) improve the functionality of, and develop, CrowdStrike's products and services, and enhance cybersecurity; and (iv) permit Customers to leverage other applications that use the data, but for all of

the foregoing, in a way that does not identify Customer or Customer's Personal Data to other customers. Neither Execution Profile/Metric Data nor Threat Actor Data are Customer's Confidential Information or Customer Data.

3. Processing Personal Data

a. Provisioning/Use of Offerings. Personal Data may be collected and used during the provisioning and use of the Offerings to deliver, support and improve the Offerings, administer the Agreement and further the business relationship between Customer and CrowdStrike, comply with law, act in accordance with Customer's written instructions, or otherwise in accordance with this Agreement. Customer authorizes CrowdStrike to collect, use, store, and transfer the Personal Data that Customer provides to CrowdStrike as contemplated in this Agreement.

b. Suspicious/Unknown File Analysis. While using certain CrowdStrike Offerings Customer may have the option to upload (by submission, configuration, and/or, in the case of Services, by CrowdStrike personnel retrieval) files and other information related to the files for security analysis and response or, when submitting crash reports, to make the product more reliable and/or improve CrowdStrike's products and services or enhance cyber-security. These potentially suspicious or unknown files may be transmitted and analyzed to determine functionality and their potential to cause instability or damage to Customer's endpoints and systems. In some instances, these files could contain Personal Data for which Customer is responsible.

4. Compliance with Privacy and Information Security Requirements

a. CrowdStrike is responsible for the security and protection of Customer Data. If utilizing a third party hosting platform, CrowdStrike remains responsible for the security and protection of Customer Data and CrowdStrike represents that its agreement with the third party hosting platform provider includes terms and conditions sufficient to allow CrowdStrike to comply with its obligations hereunder. The terms, conditions, and provisions of this Security and Data Protection section take precedence and will prevail over any other terms, conditions, and provisions of the Agreement, if in conflict. This Security and Data Protection section, including its sub-sections, survives the completion, termination, expiration, or cancellation of the Agreement. The Information Security Controls identified in Appendix 1 apply except where a higher level, more specific or additional control is required per this Exhibit A.

b. Customer solely and exclusively owns and retains all right, title and interest, whether express or implied, in and to any and all Customer Data. CrowdStrike has no and acquires no right, title or interest, whether express or implied, in and to Customer Data. CrowdStrike will only use Customer Data for the purposes set forth in the Agreement. CrowdStrike will only access Customer Data as necessary for performance of this Agreement.

c. Compliance with Laws. CrowdStrike shall comply with all Privacy and Security Laws, the EU-US Privacy Shield Framework and the Swiss-US Privacy Shield Framework as set forth by the US Department of Commerce regarding the collection, use, and retention of Personal Data from the European Economic Area, Switzerland, and the United Kingdom, as applicable. CrowdStrike's privacy notice may be found at http://www.crowdstrike.com/privacy-notice/. To the extent necessary to comply with Privacy and Security Laws, including but not limited to when Customer is a controller of Personal Data processed by CrowdStrike originating in the European Union, Switzerland, or the United Kingdom, the Data Protection Addendum set forth here https://www.crowdstrike.com/data-protection-agreement/ shall apply to CrowdStrike's processing of such Customer Personal Data.

d. Safeguards. CrowdStrike shall maintain appropriate technical and organizational safeguards commensurate with the sensitivity of the Customer Data and Personal Data processed by it on Customer's behalf, which are designed to protect the security, confidentiality, and integrity of such Customer Data and Personal Data and protect such Customer Data and Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, including the safeguards set forth on Appendix 1 which substantially conform to the ISO/IEC 27002 control framework. ("Information Security Controls for CrowdStrike Systems").

e. Access; Contacts. With respect to employees, agents, and subcontractors, CrowdStrike shall limit access to Customer Data and Personal Data to only those employees, agents, and subcontractors who have a need to access the Customer Data and/or Personal Data in order to carry out their roles as contemplated

in the terms of this Agreement.. CrowdStrike shall assign and train personnel who shall: (i) liaise with customers regarding any issues concerning the security of Customer Data and/or Personal Data; (ii) receive notice of any Security Breach discovered by CrowdStrike and provide notice of any such Security Breach to Customer; and (iii) coordinate CrowdStrike's Security Breach response and remedial action.

f. Security Program. CrowdStrike will make best efforts to protect and secure Customer Data related to this Agreement. CrowdStrike will establish and maintain an Information Security Program for GovCloud Offerings ("Program") that includes an information security policy ("Policy") applicable Offerings hosted within the boundary of the applicable FedRAMP or DISA baseline accreditation and authority to operate by the US Federal Government ("GovCloud Offerings"). CrowdStrike's Program and Policy must align with appropriate industry security frameworks and standards such as National Institute of Standards and Technology ("NIST") 800-53 Special Publication Revision 4, Federal Information Processing Standards ("FIPS") 199, or Federal Risk and Authorization Management Program ("FedRAMP"). In accordance with Section 6 of this Exhibit A, CrowdStrike will evidence of the above to Customer on a confidential, need-to-know basis, along with other related information reasonably requested by Customer regarding CrowdStrike's security practices and policies. Unless inconsistent with applicable laws, CrowdStrike and Customer must treat the Policy and related information on security practices and policies that are specific to the State as confidential information and as not public data pursuant to Minnesota Statutes section 13.37.

g. Data Management. To the extent required by the Policy, CrowdStrike will implement and maintain procedures to physically and logically segregate Customer Data. CrowdStrike will only use Customer Data to the extent necessary to perform its obligations and to improve its Offerings under the Agreement.

h. Data Encryption. When required by the Policy, CrowdStrike must encrypt all Customer Data at rest and in transit using NIST certified FIPS Publication 140-2 encryption, or applicable law, regulation or rule, whichever is a higher standard.

i. Data Center and Monitoring/Support Locations. During the term of the Agreement for GovCloud Offerings, CrowdStrike will: (1) locate all production and disaster recovery data centers that store, process or transmit Customer Data only in the continental United States, (2) store, process and transmit Customer Data only in the continental United States.

j. Security Audits & Remediation. CrowdStrike will audit the security of the CrowdStrike Systems for GovCloud Offerings, including those of the data centers used by CrowdStrike to provide such products and services. This security audit: (1) will be performed at least once every calendar year beginning with 2020; (2) will be performed according to FedRAMP requirements; (3) will be performed by third party security professionals at CrowdStrike's election and expense; (4) will result in the generation of an audit report ("CrowdStrike Audit Report"), which will, to the extent permitted by applicable law, be deemed confidential information and as not public data under the Minnesota Government Data Practices Act (Minnesota Statutes chapter 13); and (5) may be performed for other purposes in addition to satisfying this section. CrowdStrike will, in CrowdStrike's opinion, reasonably remediate or mitigate any control deficiencies identified in the CrowdStrike Audit Report in a commercially reasonable timeframe. If Customer becomes aware of any other CrowdStrike controls that do not substantially meet Customer requirements as set forth in this Exhibit A, Customer may request remediation or mitigation from CrowdStrike. CrowdStrike, in CrowdStrike's opinion, will reasonably remediate or mitigate any such control deficiencies identified by Customer or known by CrowdStrike, in a commercially reasonable timeframe.

k. Insurance and Liability. CrowdStrike will maintain the insurance described below in force and effect throughout the term of the Agreement. An Umbrella or Excess Liability insurance policy may be used to supplement CrowdStrike's policy limits to satisfy the full policy limits required by the Agreement provided that CrowdStrike warrants that the minimum coverage requirements below are met.

Professional/Technical, Errors and Omissions, including Network Security and Privacy Liability Insurance (or equivalent Network Security and Privacy Liability coverage endorsed on another form of liability coverage or written as a standalone policy):

This policy must provide coverage for all claims CrowdStrike may become legally obligated to pay resulting from any actual or alleged negligent act, error, or omission related to the Agreement, including but not

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

CrowdStrike is required to carry the following minimum limits:
$2,000,000 – per claim or event
$2,000,000 – annual aggregate

Any deductible will be the sole responsibility of the CrowdStrike and, unless CrowdStrike maintains an audited net worth of at least $100 million, the deductible may not exceed $100,000 without the written approval of Customer. If CrowdStrike desires authority from Customer to have a deductible in a higher amount, CrowdStrike shall so request in writing, specifying the amount of the desired deductible and providing financial documentation by submitting the most current audited financial statements so that Customer can ascertain the ability of CrowdStrike to cover the deductible from its own resources. The retroactive or prior acts date of such coverage shall not be after the effective date of the Agreement. Claims occurring during the term of the Agreement against such insurance may be made up to (3) years following expiration or termination of the Agreement.

CrowdStrike's policy(ies) shall be primary insurance to any other valid and collectible insurance available to Customer with respect to any claim arising out of CrowdStrike's performance under this Agreement. CrowdStrike is responsible for payment of Agreement related insurance premiums and deductibles. If CrowdStrike is self-insured, a Certificate of Self-Insurance must be provided to Customer. CrowdStrike shall obtain insurance policy(ies) from insurance company(ies) having an "AM BEST" rating of A- (minus); Financial Size Category ("FSC") VII or better, and authorized to do business in the State of Minnesota. CrowdStrike shall provide evidence of coverages meeting or exceeding the requirements of this *Insurance and Liability* Section upon Customer's request. Customer reserves the right to immediately terminate the Agreement if the CrowdStrike is not in compliance with the insurance requirements of this sub-section and retains all rights to pursue any legal remedies against the CrowdStrike.

l. Compliance with Data Privacy and Security Laws and Standards. CrowdStrike shall comply with all applicable State and federal data privacy and data security laws, rules, and regulations.

m. Criminal Justice Information Services (CJIS) Compliance: Should Customer determine a CrowdStrike Product would store, transmit or otherwise access Criminal Justice Information (CJI), upon Customer's request made prior to the purchase by Customer of such Product, the parties will meet to discuss a possible amendment to this Agreement stipulating how CrowdStrike shall comply with the applicable requirements, restrictions, and conditions set forth in the FBI Criminal Justice Information Services (CJIS) Security Policy. For the avoidance of doubt, and notwithstanding anything herein to the contrary, under no circumstances shall CrowdStrike be obligated to amend this Agreement per this clause (m).

n. Remedies. CrowdStrike acknowledges that Customer, because of the unique nature of its data, would suffer irreparable harm in the event that CrowdStrike breaches its obligation to protect the security, availability, and integrity of the Customer Data under this Exhibit A, and monetary damages may not adequately compensate Customer for such a breach. In such circumstances, Customer will be entitled, in addition to monetary relief, to injunctive relief or specific performance as may be necessary to restrain any continuing or further breach by CrowdStrike, without showing or proving any actual damages sustained by Customer.

o. Business Continuity. CrowdStrike shall have written business continuity and disaster recovery plans that define the roles, responsibilities and procedures necessary to ensure that products and services provided under this Agreement shall be maintained continuously in the event of a disruption to CrowdStrike's operations, regardless of the cause of the disruption. Such plans must, at a minimum, define CrowdStrike's actions to address the impacts of the following key areas likely to cause a disruption to CrowdStrike's operations: loss of key personnel, loss of facility, and loss of information technology. CrowdStrike must conduct testing and review of its business continuity and disaster recovery plan at least annually.

p. Background Checks. CrowdStrike agrees and acknowledges that all CrowdStrike personnel performing Offerings under this Agreement have undergone background screening, including: (i) Criminal Records

Search: County Felony and Misdemeanor Criminal Records Search: Federal Standard Criminal; (ii) Civil Records Search: County Civil; (iii) Social Security Number Death Master Search Motor Vehicle Records Credit Report; (iv) Bankruptcy Records Search; (v) Sex Offender Registry Search (if applicable); (vi) Government Registries Search; and (vii) Education and Employment. Verification If any provision of this sub-section is found to violate any applicable laws, rules, or State policies, then CrowdStrike will be relieved of all obligations arising under such provision. Notwithstanding anything to the contrary in this sub-section, this sub-section is only applicable and effective to extent that it is consistent with applicable laws, rules, and State policies

5. **Security Breach, Security Incident and Privacy Incident Response**
In the event CrowdStrike discovers a Security Breach, Security Incident, or Privacy Incident, CrowdStrike shall:
   a. Without undue delay but no later than 48 hours of becoming aware, notify Customer of the discovery of Security Breach, Security Incident, or Privacy Incident. Such notice shall summarize the known circumstances of the Security Incident or Privacy Incident and the corrective action taken or to be taken by CrowdStrike.
   b. Conduct an investigation of the circumstances of the Security Incident, or Privacy Incident.
   c. Use commercially reasonable efforts to remediate the Security Incident, or Privacy Incident.
   d. Use commercially reasonable efforts to communicate and cooperate with Customer concerning its response to the Security Breach, Security Incident, or Privacy Incident.
   e. The decision to notify the affected data subjects in a way that identifies the Customer's involvement and the form of such notice following report of a Security Breach, Security Incident, or Privacy Incident under this Section are the responsibility of the Customer, as allowed for under applicable law.

6. **Security Assessment and Provision of Audited Security Controls**. Promptly after written (including email) request from Customer, CrowdStrike shall provide Customer with: (i) its most recent SOC II, Type 2 report regarding the CrowdStrike Systems; and (ii) provide its completed Standardized Information Gathering (SIG) questionnaire (or similar document) for the CrowdStrike Systems (the "Security Documentation"). Upon the provision of reasonable notice to CrowdStrike, once every twelve months during the term of the Agreement and during normal business hours unless otherwise decided by CrowdStrike in its sole discretion, CrowdStrike shall make appropriate CrowdStrike personnel reasonably available to Customer to discuss CrowdStrike's manner of compliance with applicable security obligations under this Agreement. In advance of such discussion, CrowdStrike may, in addition to the Security Documentation, provide Customer with access to additional requested information or documentation concerning CrowdStrike's information security practices as they relate to this Agreement, including without limitation, access to any security assessment reports designed to be shared with third parties. Any information or documentation provided pursuant to this assessment process or otherwise pursuant to this Schedule shall be considered CrowdStrike's Confidential Information and subject to the Confidentiality section of the Agreement.

7. **Customer Obligations**. Customer, along with its Affiliates, represents and warrants that: (i) it owns or has a right of use from a third party, and controls, directly or indirectly, all of the software, hardware and computer systems (collectively, "Systems") where the Products and/or CrowdStrike Tools will be installed or that will be the subject of, or investigated during, the Offerings, (ii) to the extent required under any federal, state, or local U.S. or non-US laws (e.g., Computer Fraud and Abuse Act, 18 U.S.C. § 1030 et seq., Title III, 18 U.S.C. 2510 et seq., and the Electronic Communications Privacy Act, 18 U.S.C. § 2701 et seq.) it has authorized CrowdStrike to access the Systems and process and transmit data through the Offerings and CrowdStrike Tools in accordance with this Agreement and as necessary to provide and perform the Offerings, (iii) it has a lawful basis in having CrowdStrike investigate the Systems, process the Customer Data and the Personal Data; (iv) that it is and will at all relevant times remain duly and effectively authorized to instruct CrowdStrike to carry out the Offerings, and (v) it has made all necessary disclosures, obtained all necessary consents and government authorizations required under applicable law to permit the processing and international transfer of Customer Data and Customer Personal Data from each Customer and Customer Affiliate, to CrowdStrike.

8. **Notices**. The following individuals shall be the primary contacts at Customer and CrowdStrike for any coordination, communications or notices with respect to Personal Data and this Schedule:

a. **CrowdStrike:** Drew Bagley, VP & Counsel, Privacy & Cyber Policy (drew.bagley@crowdstrike.com with a copy to legal@crowdstrike.com). For any Security Breach: Jerry Dixon, Chief Information Security Officer (jerry.dixon@crowdstrike.com with a copy to security@crowdstrike.com).
b. **Customer:** the person who has signed the Agreement or another person as otherwise designated in writing (including by email) by Customer to CrowdStrike. Each party shall promptly notify the other if any of the foregoing contact information changes.

Appendix 1
Information Security Controls for CrowdStrike Systems

Security Control Category	Description
1. Governance	a. Assign to an individual or a group of individuals appropriate roles for developing, coordinating, implementing, and managing CrowdStrike's administrative, physical, and technical safeguards designed to protect the security, confidentiality, and integrity of Personal Data b. Use of data security personnel that are sufficiently trained, qualified, and experienced to be able to fulfill their information security-related functions
2. Risk Assessment	a. Conduct periodic risk assessments designed to analyze existing information security risks, identify potential new risks, and evaluate the effectiveness of existing security controls b. Maintain risk assessment processes designed to evaluate likelihood of risk occurrence and material potential impacts if risks occur c. Document formal risk assessments d. Review formal risk assessments by appropriate managerial personnel
3. Information Security Policies	a. Create information security policies, approved by management, published and communicated to all employees and relevant external parties. b. Review policies at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.
4. Human Resources Security	a. Maintain policies requiring reasonable background checks of any new employees who will have access to Personal Data or relevant CrowdStrike Systems, subject to local law b. Regularly and periodically train personnel on information security controls and policies that are relevant to their business responsibilities and based on their roles within the organization
5. Asset Management	a. Maintain policies establishing data classification based on data criticality and sensitivity b. Maintain policies establishing data retention and secure destruction requirements c. Implement procedures to clearly identify assets and assign ownership
6. Access Controls	a. Identify personnel or classes of personnel whose business functions and responsibilities require access to Personal Data, relevant CrowdStrike Systems and the organization's premises b. Maintain controls designed to limit access to Personal Data, relevant CrowdStrike Systems and the facilities hosting the CrowdStrike Systems to authorized personnel c. Review personnel access rights on a regular and periodic basis d. Maintain physical access controls to facilities containing CrowdStrike Systems, including by using access cards or fobs issued to CrowdStrike personnel as appropriate e. Maintain policies requiring termination of physical and electronic access to Personal Data and CrowdStrike Systems after termination of an employee f. Implement access controls designed to authenticate users and limit access to CrowdStrike Systems g. Implement policies restricting access to the data center facilities hosting CrowdStrike Systems to approved data center personnel and limited and approved CrowdStrike personnel h. Maintain dual layer access authentication processes for CrowdStrike employees with administrative access rights to CrowdStrike Systems
7. Cryptography	a. Implement encryption key management procedures b. Encrypt sensitive data using a minimum of AES/128 bit ciphers in transit and at rest
8. Physical Security	a. Require two factor controls to access office premises b. Register and escort visitors on premises
9. Operations Security	a. Perform periodic network and application vulnerability testing using dedicated qualified internal resources b. Contract with qualified independent 3rd parties to perform periodic network and application penetration testing c. Implement procedures to document and remediate vulnerabilities discovered during vulnerability and penetration tests

10. Communications Security	a. Maintain a secure boundary using firewalls and network traffic filtering b. Require internal segmentation to isolate critical systems from general purpose networks c. Require periodic reviews and testing of network controls
11. System Acquisition, Development and Maintenance	a. Assign responsibility for system security, system changes and maintenance b. Test, evaluate and authorize major system components prior to implementation
12. Supplier Relationships	Periodically review available security assessment reports of vendors hosting the CrowdStrike Systems to assess their security controls and analyze any exceptions set forth in such reports
13. Information Security Breach Management	a. Monitor the access, availability, capacity and performance of the CrowdStrike Systems, and related system logs and network traffic using various monitoring software and services b. Maintain incident response procedures for identifying, reporting, and acting on Security Breaches c. Perform incident response table-top exercises with executives and representatives from across various business units d. Implement plan to address gaps discovered during exercises e. Establish a cross-disciplinary Security Breach response team
14. Business Continuity Management	a. Design business continuity with goal of 99.9% uptime SLA b. Conduct scenario based testing annually
15. Compliance	a. Establish procedures designed to ensure all applicable statutory, regulatory and contractual requirements are adhered to

Exhibit B – CrowdStrike Competitors

Appthority Bitdefender Broadcom/Symantec
Check Point (SandBlast) Cisco (AMP)
Comodo Cybereason Blackberry/Cylance Digital Guardian Elastic/Endgame enSilo
ESET
F-secure
Fidelis Cybersecurity Fireeye
FlashPoint Forcepoint Fortinet
Joe Security Kaspersky Lastline McAfee
Microsoft (Windows Defender Advanced Threat Protection) Palo Alto (Traps)
Panda Security Rapid7 SentinelOne Sophos Tanium Tenable
Trend Micro VMRay
VMWare/Carbon Black Webroot
Ziften Zimperium