SUBMITTAL TO THE RIVERSIDE UNIVERSITY HEALTH SYSTEM MEDICAL CENTER GOVERNING BOARD COUNTY OF RIVERSIDE, STATE OF CALIFORNIA

ITEM: 18.4
(ID # 28010)
MEETING DATE:
Tuesday, June 10, 2025

FROM : RUHS-MEDICAL CENTER

SUBJECT: RIVERSIDE UNIVERSITY HEALTH SYSTEM - MEDICAL CENTER: Approve and Execute the Master Agreement with CrowdStrike and authorize the purchase of CrowdStrike Falcon Endpoint Protection Software through CDWG for three (3) years effective upon signature; All Districts. [Total Cost $2,100,000; up to $210,000 in Additional Compensation - 100% Hospital Enterprise Fund]

RECOMMENDED MOTION: That the Board of Supervisors:

1. Approve the Master Agreement with CrowdStrike for the purchase of CrowdStrike Falcon Endpoint Protection Software ("Agreement") for a total amount of $2,100,000, for three (3) years effective upon signature, and authorize the Chair of the Board to sign the Agreement on behalf of the County; and
2. Authorize the Purchasing Agent, in accordance with Ordinance No. 459 and based on the availability of fiscal funding and as approved as to form by County Counsel, to: (a) sign amendments including modifications to the statement of work that stay within the intent of the Agreement and (b) sign amendments to the compensation provisions that do not exceed sum total of ten percent (10%) of the total cost of the Agreement.
3. Authorize the Purchasing Agent to issue Purchase Order(s) to CDW-Government in an amount not to exceed $2,310,000 for the goods and services described in motion 1 and consistent with the Board's approval.

ACTION:Policy

Jennifer Cruikshank
Jennifer Cruikshank, Chief Executive Officer – Health System 5/27/2025

MINUTES OF THE GOVERNING BOARD

On motion of Supervisor Gutierrez, seconded by Supervisor Washington and duly carried by unanimous vote, IT WAS ORDERED that the above matter is approved as recommended.

Ayes:	Medina, Spiegel, Washington, Perez and Gutierrez
Nays:	None
Absent:	None
Date:	June 10, 2025
xc:	RUHS-MC

Kimberly A. Rector
Clerk of the Board
By: _____ Deputy

SUBMITTAL TO THE RIVERSIDE UNIVERSITY HEALTH SYSTEM MEDICAL CENTER GOVERNING BOARD OF DIRECTORS COUNTY OF RIVERSIDE, STATE OF CALIFORNIA

FINANCIAL DATA	Current Fiscal Year:	Next Fiscal Year:	Total Cost:	Ongoing Cost
COST	$450,000	$825,000	$2,100,000	$0
NET COUNTY COST	$0	$0	$0	$0
SOURCE OF FUNDS: 100% Hospital Enterprise Fund - 40050			Budget Adjustment: No	
			For Fiscal Year: 24/25-27/28	

C.E.O. RECOMMENDATION: Approve

BACKGROUND:

Summary

Riverside University Health System - Information Services (RUHS-IS) is requesting approval to procure the CrowdStrike Falcon Endpoint Protection solution through CDW-Government to improve its cybersecurity posture. The primary goal of this initiative is to enhance continuous round-the-clock monitoring of potential security threats across all systems within RUHS-MC.

The CrowdStrike Falcon Platform is a state-of-the-art, cloud-based software as a service (SaaS) application designed to deliver advanced endpoint protection. This solution will be deployed across all RUHS endpoints, including computers, servers, laptops, and PCs, and includes a lightweight object code sensor that will be installed locally on each device.

Key features of the CrowdStrike Falcon Platform include:

- Advanced Malware Detection: The Falcon platform enables the identification of previously unknown malware, including sophisticated zero-day threats.
- Real-Time Protection: The software is designed to detect and prevent attacks in real-time, reducing the potential for system damage or data loss.
- Threat Intelligence and Attribution: The system allows for the identification of advanced adversaries and provides attribution of attacks, which is critical in understanding the nature of threats and preventing future incidents.
- 24/7 Monitoring and Managed Threat Response: With Falcon Complete, the platform provides comprehensive management and a managed threat response service that operates around the clock, ensuring that any potential threats are addressed promptly.

The integration of this solution is crucial to improving the security infrastructure at RUHS-MC, safeguarding sensitive patient data, and ensuring the continued operation of the health system's IT infrastructure. Given the increased frequency and sophistication of cyberattacks targeting healthcare institutions, the ability to maintain continuous monitoring and swift response capabilities is essential for mitigating risks.

SUBMITTAL TO THE RIVERSIDE UNIVERSITY HEALTH SYSTEM MEDICAL CENTER GOVERNING BOARD OF DIRECTORS COUNTY OF RIVERSIDE, STATE OF CALIFORNIA

Approval of this agreement will enhance the cybersecurity framework at RUHS-MC by providing robust, real-time protection against the increasing risk of cyber threats, thereby ensuring the safeguard of critical systems and patient data.

If Board of Supervisors approval is granted, RUHS-MC seeks to leverage cooperative agreement number 2024056-01 between Omnia Partners and CDW Government LLC. Omnia Partners is a cooperative purchasing agency that is available to all government and educational entities and competitively solicited this agreement using the Request for Proposal (RFP) method by means of solicitation number 2024056. Through this solicitation it was determined that CDW Government LLC is the most qualified and responsive bidder as Reseller of Information Technology Solutions Products and Services.

Impact on Residents and Businesses

These services are a component of RUHS-MC's system of care aimed at improving the health and safety of its patients and the community.

Contract History and Price Reasonableness

The Agreement that was leveraged between Omnia Partners and CDW Government LLC, Contract Number 2024056-01, has been competitively bid out utilizing the Request for Proposal (RFP#2024056) method of procurement. This agreement was entered into on July 5, 2024 and is effective July 2, 2024 through July 1, 2028.

This Agreement requires Board approval as the compensation provision exceeds the Purchasing Agent's authority and $100,000 threshold for contracting with a vendor for professional services per Purchasing Policy Manual, County Ordinance 459 and California Government Code § 25502.5.

ATTACHMENTS:

Attachment A: CrowdStrike Master Agreement
Attachment B: Business Associate Agreement
Attachment C: RUHS Crowdstrike three (3) Year Quote

Melissa Curtis
Melissa Curtis, Deputy Director of Purchasing and Fleet 5/23/2025

Jacqueline Ruiz
Jacqueline Ruiz, Principal Analyst 6/5/2025

Gregg Gu
Gregg Gu, Chief of Deputy County Counsel 5/27/2025

HIPAA Business Associate Agreement
Between the County of Riverside and CrowdStrike, Inc.

This HIPAA Business Associate Agreement (the "Addendum") supplements, and is made part of the CrowdStrike Master Agreement Terms and Conditions (the "Underlying Agreement") between the County of Riverside ("County") and CrowdStrike, Inc. ("Contractor") and shall be effective as of the date the Underlying Agreement is approved by both Parties (the "Effective Date").

RECITALS

WHEREAS, County and Contractor entered into the Underlying Agreement pursuant to which the Contractor provides services to County, and in conjunction with the provision of such services certain protected health information ("PHI") and/or certain electronic protected health information ("ePHI") may be created by or made available to Contractor for the purposes of carrying out its obligations under the Underlying Agreement; and,

WHEREAS, the provisions of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Public Law 104-191 enacted August 21, 1996, and the Health Information Technology for Economic and Clinical Health Act ("HITECH") of the American Recovery and Reinvestment Act of 2009, Public Law 111-5 enacted February 17, 2009, and the laws and regulations promulgated subsequent thereto, as may be amended from time to time, are applicable to the protection of any use or disclosure of PHI and/or ePHI pursuant to the Underlying Agreement; and,

WHEREAS, County is a covered entity, as defined in the Privacy Rule; and,

WHEREAS, to the extent County discloses PHI and/or ePHI to Contractor or Contractor creates, receives, maintains, transmits, or has access to PHI and/or ePHI of County, Contractor is a business associate, as defined in the Privacy Rule; and,

WHEREAS, pursuant to 42 USC §17931 and §17934, certain provisions of the Security Rule and Privacy Rule apply to a business associate of a covered entity, the additional security and privacy requirements of HITECH may be applicable to business associates and must be incorporated into the business associate agreement where required by applicable law, and a business associate may be liable for civil and criminal penalties for failure to comply with these security and/or privacy provisions; and,

WHEREAS, the parties mutually agree that any use or disclosure of PHI and/or ePHI must be in compliance with the Privacy Rule, Security Rule, HIPAA, HITECH and any other applicable law; and,

WHEREAS, the parties intend to enter into this Addendum to address the requirements and obligations set forth in the Privacy Rule, Security Rule, HITECH and HIPAA as they apply to Contractor as a business associate of County, including the establishment of permitted and required uses and disclosures of PHI and/or ePHI created or received by Contractor during the course of performing functions, services and activities on behalf of County, and appropriate limitations and conditions on such uses and disclosures;

NOW, THEREFORE, in consideration of the mutual promises and covenants contained herein, the parties agree as follows:

1. Definitions. Terms used, but not otherwise defined, in this Addendum shall have the same meaning as those terms in HITECH, HIPAA, Security Rule and/or Privacy Rule, as may be amended from time to time.

   A. "Breach" when used in connection with PHI means the acquisition, access, use or disclosure of PHI in a manner not permitted under subpart E of the Privacy Rule which compromises the security or privacy of the PHI, and shall have the meaning given such term in 45 CFR §164.402.

      (1) Except as provided below in Paragraph (2) of this definition, acquisition, access, use, or

disclosure of PHI in a manner not permitted by subpart E of the Privacy Rule is presumed to be a breach unless Contractor demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following four factors:

(a) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

(b) The unauthorized person who used the PHI or to whom the disclosure was made;

(c) Whether the PHI was actually acquired or viewed; and

(d) The extent to which the risk to the PHI has been mitigated.

(2) Breach excludes:

(a) Any unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of a covered entity or business associate, if such acquisition, access or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of the Privacy Rule.

(b) Any inadvertent disclosure by a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity, business associate, or organized health care arrangement in which County participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted by subpart E of the Privacy Rule.

(c) A disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

B. "Business associate" has the meaning given such term in 45 CFR § 160.103, including but not limited to a subcontractor that creates, receives, maintains, transmits or accesses PHI on behalf of the business associate.
C. "Data aggregation" has the meaning given such term in 45 CFR §164.501.
D. "Designated record set" as defined in 45 CFR §164.501 means a group of records maintained by or for a covered entity that may include: the medical records and billing records about individuals maintained by or for a covered health care provider; the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or, used, in whole or in part, by or for the covered entity to make decisions about individuals.
E. "Electronic protected health information" ("ePHI") as defined in 45 CFR §160.103 means protected health information transmitted by or maintained in electronic media.
F. "Health care operations" has the meaning given such term in 45 CFR §164.501.
G. "Individual" as defined in 45 CFR §160.103 means the person who is the subject of protected health information.
H. "Part II" means the Federal Confidentiality of Alcohol and Drug Abuse Patient Records law and regulations set forth at 42 U.S.C. § 290dd-2 and 42 C.F.R. Part II.
I. "Person" as defined in 45 CFR §160.103 means a natural person, trust or estate, partnership, corporation, professional association or corporation, or other entity, public or private.
J. "Privacy Rule" means the HIPAA regulations codified at 45 CFR Parts 160 and 164, Subparts A and E.
K. "Protected health information" ("PHI") has the meaning given such term in 45 CFR §160.103, which includes ePHI.
L. "Qualified Service Organization" means a person or entity that provides services to a Part II program, such as data processing, bill collecting, dosage preparation, laboratory analyses, or legal, accounting, population health management, medical staffing, or other professional services, or services to prevent or treat child abuse or neglect, including training on nutrition and child care and individual and group therapy and has entered into an agreement with a Part II program

M. "Required by law" has the meaning given such term in 45 CFR §164.103.
N. "Secretary" means the Secretary of the U.S. Department of Health and Human Services ("HHS").
O. "Security incident" as defined in 45 CFR §164.304 means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.
P. "Security Rule" means the HIPAA Regulations codified at 45 CFR Parts 160 and 164, Subparts A and C.
Q. "Subcontractor" as defined in 45 CFR §160.103 means a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.
R. "Unsecured protected health information" and "unsecured PHI" as defined in 45 CFR §164.402 means PHI not rendered unusable, unreadable, or indecipherable to unauthorized persons through use of a technology or methodology specified by the Secretary in the guidance issued under 42 USC §17932(h)(2).

2. Scope of Use and Disclosure by Contractor of County's PHI and/or ePHI.

A. Except as otherwise provided in this Addendum, Contractor may use, disclose, or access PHI and/or ePHI as necessary to perform any and all obligations of Contractor under the Underlying Agreement or to perform functions, activities or services for, or on behalf of, County as specified in this Addendum, if such use or disclosure does not violate HIPAA, HITECH, the Privacy Rule and/or Security Rule.
B. Unless otherwise limited herein, in addition to any other uses and/or disclosures permitted or authorized by this Addendum, the Underlying Agreement or required by law, in accordance with 45 CFR §164.504(e)(2), Contractor may:
    1) Use PHI and/or ePHI if necessary for Contractor's proper management and administration and to carry out its legal responsibilities; and,
    2) Disclose PHI and/or ePHI for the purpose of Contractor's proper management and administration or to carry out its legal responsibilities, only if:
        a) The disclosure is required by law; or,
        b) Contractor obtains reasonable assurances, in writing, from the person to whom Contractor will disclose such PHI and/or ePHI that the person will:
            i. Hold such PHI and/or ePHI in confidence and use or further disclose it only for the purpose for which Contractor disclosed it to the person, or as required by law; and,
            ii. Notify Contractor of any instances of which it becomes aware in which the confidentiality of the information has been breached; and,
    3) Use PHI to provide data aggregation services relating to the health care operations of County pursuant to the Underlying Agreement or as requested by County; and,
    4) De-identify all PHI and/or ePHI of County received by Contractor under this Addendum provided that the de-identification conforms to the requirements of the Privacy Rule and/or Security Rule.
C. Notwithstanding the foregoing, to the extent state and/or federal laws and/or regulations are directly applicable to Contractor's performance under this Agreement as a business associate which are more stringent in their requirements than the provisions of HIPAA the applicable state and/or federal laws and/or regulations shall control the disclosure of records.
D. Part II Provisions
    a. To the extent that in performing its services for or on behalf of County, Contractor uses, discloses, maintains, or transmits PHI that is protected by Part II, Contractor acknowledges and agrees that it is a Qualified Service Organization for the purpose of such federal law; acknowledges and agrees that in receiving, storing, processing or otherwise dealing with any such patient records, it is fully bound by the Part II regulations; and, if necessary will resist in judicial proceedings any efforts to obtain access to patient records except as permitted by the Part II regulation.
    b. Notwithstanding any other language in this Agreement, Contractor acknowledges and agrees that any patient information it receives from County that is protected by Part II is subject to protections that prohibit Contractor from disclosing such information to

agents or subcontractors without the specific, prior written consent of County. The parties hereby acknowledge and agree that execution of this Agreement and the Underlying Agreement constitute such consent for Contractor to disclose such information to subprocessors or Subcontractors as provided for in the Underlying Agreement (including the Data Protection Addendum).

c. Without limiting any of Contractor's obligations under this Section, County hereby agrees to use commercially reasonable efforts not to give or provide Contractor with access to any PHI that is protected by Part II.

3. Prohibited Uses and Disclosures.
   A. Contractor may neither use, disclose, nor access PHI and/or ePHI in a manner not authorized by the Underlying Agreement or this Addendum without authorization in writing from County.
   B. Contractor may neither use, disclose, nor access PHI and/or ePHI it receives from County or from another business associate of County, except as permitted or required by this Addendum, the Underlying Agreement, or as required by law.
   C. Contractor agrees not to make any disclosure of PHI and/or ePHI that County would be prohibited from making as a covered entity under Subpart E of 45 CFR Part 164.
   D. Contractor shall not use or disclose PHI for any purpose prohibited by the Privacy Rule, Security Rule, HIPAA and/or HITECH, including, but not limited to 42 USC §17935 and §17936. Contractor agrees:
      1) Not to use or disclose PHI for fundraising, unless pursuant to the Underlying Agreement and only if permitted by and in compliance with the requirements of 45 CFR §164.514(f) or 45 CFR §164.508;
      2) Not to use or disclose PHI for marketing, as defined in 45 CFR §164.501, unless pursuant to the Underlying Agreement and only if permitted by and in compliance with the requirements of 45 CFR §164.508(a)(3);
      3) Not to disclose PHI, except as otherwise required by law, to a health plan for purposes of carrying out payment or health care operations, if the individual has requested this restriction pursuant to 42 USC §17935(a) and 45 CFR §164.522, and has paid out of pocket in full for the health care item or service to which the PHI solely relates; and,
      4) Not to receive, directly or indirectly, remuneration in exchange for PHI, or engage in any act that would constitute a sale of PHI, as defined in 45 CFR §164.502(a)(5)(ii), unless permitted by the Underlying Agreement and in compliance with the requirements of a valid authorization under 45 CFR §164.508(a)(4). This prohibition shall not apply to payment by County to Contractor for services provided pursuant to the Underlying Agreement. For the avoidance of doubt, Neither Execution Profile/Metric Data nor Threat Actor Data, as defined in the Underlying Agreement are Customer's PHI.

4. Obligations of County.
   A. County agrees to make its best efforts to notify Contractor promptly in writing of any restrictions on the use or disclosure of PHI and/or ePHI agreed to by County that may affect Contractor's ability to perform its obligations under the Underlying Agreement, or this Addendum.
   B. County agrees to make its best efforts to promptly notify Contractor in writing of any changes in, or revocation of, permission by any individual to use or disclose PHI and/or ePHI, if such changes or revocation may affect Contractor's ability to perform its obligations under the Underlying Agreement, or this Addendum.
   C. County agrees to make its best efforts to promptly notify Contractor in writing of any known limitation(s) in its notice of privacy practices to the extent that such limitation may affect Contractor's use or disclosure of PHI and/or ePHI.
   D. County agrees not to request Contractor to use or disclose PHI and/or ePHI in any manner that would not be permissible under HITECH, HIPAA, the Privacy Rule, and/or Security Rule.
   E. County agrees to obtain any authorizations necessary for the use or disclosure of PHI

and/or ePHI, so that Contractor can perform its obligations under this Addendum and/or Underlying Agreement.

5. Obligations of Contractor. In connection with the use or disclosure of PHI and/or ePHI, Contractor agrees to:
   A. Use or disclose PHI only if such use or disclosure complies with each requirement of 45 CFR §164.504(e) applicable to a business associate. Contractor shall also comply with the additional privacy requirements that are applicable to business associates in HITECH, as may be amended from time to time.
   B. Not use or further disclose PHI and/or ePHI other than as permitted or required by this Addendum, the Underlying Agreement or as required by law. To the extent permissible under applicable law, Contractor will notify County if Contractor is required by law to disclose PHI and/or ePHI.
   C. Use appropriate safeguards and comply, where applicable, with the Security Rule with respect to ePHI, to prevent use or disclosure of PHI and/or ePHI other than as provided for by this Addendum or the Underlying Agreement.
   D. Mitigate, to the extent practicable, any harmful effect that is known to Contractor of a use or disclosure of PHI and/or ePHI by Contractor in violation of this Addendum.
   E. Report to County any use or disclosure of PHI and/or ePHI not provided for by this Addendum or otherwise in violation of HITECH, HIPAA, the Privacy Rule, and/or Security Rule of which Contractor becomes aware, including Breaches of unsecured PHI as required by 45 CFR §164.410.
   F. In accordance with 45 CFR §164.502(e)(1)(ii), require that any subcontractors that create, receive, maintain, transmit or access PHI on behalf of the Contractor agree through contract to the same restrictions and conditions that apply to Contractor with respect to such PHI and/or ePHI, including the restrictions and conditions pursuant to this Addendum.
   G. To the extent required by law, ordinance, or statute make available to the Secretary Contractor's internal practices, books and records relating to the use, disclosure and privacy protection of PHI received from County, or created or received by Contractor on behalf of County, for purposes of determining compliance with the Privacy Rule.
   H. Request, use or disclose only the minimum amount of PHI necessary to accomplish the intended purpose of the request, use or disclosure in accordance with 42 USC §17935(b) and 45 CFR §164.502(b)(1).
   I. If CrowdStrike receives a third-party subpoena or request for the production of PHI, whether valid or not, to the extent permissible by law, CrowdStrike agrees to provide RUHS with reasonable notice of both the request and CrowdStrike's intended response.
   J. Use appropriate administrative, technical and physical safeguards to prevent unauthorized use, disclosure, or access of PHI and/or ePHI.
   K. Obtain and maintain knowledge of applicable laws and regulations related to HIPAA and HITECH, as may be amended from time to time.
   L. Comply with the requirements of the Privacy Rule that apply to the County to the extent Contractor is to carry out County's obligations under the Privacy Rule.
   M. Take reasonable steps to cure or end any pattern of activity or practice of its subcontractor of which Contractor becomes aware that constitute a material breach or violation of the subcontractor's obligations under the business associate contract with Contractor, and if such steps are unsuccessful, Contractor agrees to terminate its contract with the subcontractor if feasible.

6. Access to PHI, Amendment and Disclosure Accounting. Contractor agrees to:
   A. Access to PHI, including ePHI. Make available PHI, including ePHI if maintained electronically, in a designated record set to County or as directed by County to satisfy the requirements of 45 CFR §164.524.
   B. Amendment of PHI. Make PHI amendments to PHI in a designated record set County directs or as agreed to by County as necessary to satisfy County's obligations under 45 CFR §164.526.

C. Accounting of disclosures of PHI. Maintain and make available the information required to provide an accounting of disclosures to County to satisfy its obligations to provide accounting of disclosures of PHI under 45 CFR §164.528. Contractor shall:
   1) Document such disclosures of PHI, and information related to such disclosures, as would be required for County to respond to a request by an individual for an accounting of disclosures of PHI in accordance with 45 CFR §164.528.
   2) Make available to County information collected in accordance with this section to permit County to respond to a request by an individual for an accounting of disclosures of PHI.
   3) To the extent available, make available for County information required by this Section 6.C for the six (6) years preceding the individual's request for accounting of disclosures of PHI.

7. Security of ePHI. In the event County discloses ePHI to Contractor or Contractor needs to create, receive, maintain, transmit or have access to County ePHI, in accordance with 42 USC §17931 and 45 CFR §164.314(a)(2)(i), and §164.306, Contractor shall, to the extent directly applicable to a business associate:
   1. Comply with the applicable requirements of the Security Rule, and implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of ePHI that Contractor creates, receives, maintains, or transmits on behalf of County in accordance with 45 CFR §164.308, §164.310, and §164.312;
   2. Comply with each of the requirements of 45 CFR §164.316 directly applicable to a business associate relating to the implementation of policies, procedures and documentation requirements with respect to ePHI;
   3. Protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI;
   4. Protect against any reasonably anticipated uses or disclosures of ePHI that are not permitted or required under the Privacy Rule;
   5. Ensure compliance with the Security Rule by Contractor's workforce, to the extent and in the manner that the Security Rule is applicable to Contractor's workforce; In accordance with 45 CFR §164.308(b)(2), require that any subcontractors that create, receive, maintain, transmit, or access ePHI on behalf of Contractor agree through contract to the same restrictions and requirements contained in this Addendum;
   6. Report to County any security incident of which Contractor becomes aware, including breaches of unsecured PHI as required by 45 CFR §164.410; and,

8. Breach of Unsecured PHI. In the case of breach of unsecured PHI, Contractor shall comply with the provisions of 42 USC §17932 and 45 CFR Part 164, Subpart D, including but not limited to 45 CFR §164.410 applicable to a business associate.
   A. Discovery and notification. Following the discovery of a breach of unsecured PHI, Contractor shall notify County in writing of such breach without unreasonable delay and in no case later than 60 calendar days after discovery of a breach, except as provided in 45 CFR §164.412.
      1) Breaches treated as discovered. A breach is treated as discovered by Contractor as of the first day on which such breach is known to Contractor or, by exercising reasonable diligence, would have been known to Contractor, which includes any person, other than the person committing the breach, who is an employee, officer, or other agent of Contractor (determined in accordance with the federal common law of agency).
      2) Content of notification. The written notification to County relating to breach of unsecured PHI shall include, to the extent possible, the following information if known (or can be reasonably obtained) by Contractor:
         a) The identification of each individual whose unsecured PHI has been, or is reasonably believed by Contractor to have been accessed, acquired, used or disclosed during the breach;

b) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
c) A description of the types of unsecured PHI involved in the breach, such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved;
d) Any steps individuals should take to protect themselves from potential harm resulting from the breach;
e) A brief description of what Contractor is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches.

B. Additional Information. With respect to any Breach of unsecured PHI reported by Contractor, Contractor shall provide County with all necessary information that County is required to include in its notification obligations, under 45 CFR §164.410 as information becomes available.

C. Delay of notification authorized by law enforcement. If Contractor delays notification of breach of unsecured PHI pursuant to a law enforcement official's statement that required notification, notice or posting would impede a criminal investigation or cause damage to national security, Contractor shall maintain documentation sufficient to demonstrate its compliance with the requirements of 45 CFR §164.412.

D. Payment of costs. With respect to any breach of unsecured PHI caused solely by the Contractor's failure to comply with one or more of its obligations under this Addendum and/or the provisions of HITECH, HIPAA, the Privacy Rule or the Security Rule, subject to the Specified Damages Cap in the Underlying Agreement and upon request of County, Contractor agrees to pay any and all costs associated with providing all legally required notifications to individuals, media outlets, and the Secretary. The Parties agree that the total combined liability of either Party and its Affiliates toward the other Party and its Affiliates under or in connection with this Agreement and the Underlying Agreement combined will be as set forth in the Underlying Agreement.

E. Documentation. Pursuant to 45 CFR §164.414(b), to the extent and in the manner directly applicable to Contractor's performance under the Underlying Agreement, in the event Contractor's use or disclosure of PHI and/or ePHI violates the Privacy Rule, Contractor shall maintain documentation sufficient to demonstrate that all notifications were made by Contractor as required by 45 CFR Part 164, Subpart D, or that such use or disclosure did not constitute a breach, including Contractor's completed risk assessment and investigation documentation.

F. Additional State Reporting Requirements. The parties agree that this Section 8.F applies only if and/or when County, in its capacity as a licensed clinic, health facility, home health agency, or hospice, is required to report unlawful or unauthorized access, use, or disclosure of medical information under the more stringent requirements of California Health & Safety Code §1280.15.
1) Contractor agrees to reasonably assist County to fulfill its reporting obligations to affected patients and to the California Department of Public Health ("CDPH") in a timely manner under the California Health & Safety Code §1280.15.
2) Contractor reasonably agrees to notify County of any unauthorized access, use, or disclosure of patient medical information provided to Contractor by County after Contractor becomes aware of such incident. Contractor further agrees such notification shall be made in writing, and shall include substantially the same types of information listed above in Section 8.A.2 (Content of Notification) as applicable to the unauthorized access, use, or disclosure.

9. Indemnification. For the avoidance of doubt, the indemnification obligations of the Underlying Agreement remain fully applicable to this BAA and are incorporated herein by reference as set forth in Section 9 of the Underlying Agreement.
10. Term. This Addendum shall commence upon the Effective Date and shall terminate when all PHI and/or ePHI provided by County to Contractor, or created or received by Contractor on behalf of County, is destroyed or returned to County, or, if it is infeasible to return or destroy PHI and/ePHI, protections are extended to such information, in accordance with section 11.B of this Addendum.
11. Termination.

A. Termination for Breach of Contract. A material breach of any provision of this Addendum by either party shall constitute a material breach of the Underlying Agreement and will provide grounds for terminating this Addendum and the Underlying Agreement. Either party, upon written notice to the other party describing the breach, may take any of the following actions:
   1) Terminate the Underlying Agreement and this Addendum, upon written notification to the other party, if the other party breaches a material provision of this Addendum and the terminating party has reasonably determined curing such breach is not feasible.
   2) Provide the other party with an opportunity to cure the alleged material breach and in the event the other party fails to cure the breach to the satisfaction of the non-breaching party within thirty (30) days' notice of such a breach the non-breaching party has the right to immediately terminate the Underlying Agreement and this Addendum.

B. Effect of Termination.
   1) Upon termination of this Addendum, for any reason, Contractor shall return or destroy all PHI and/or ePHI received from County, or created or received by the Contractor on behalf of County, and, in the event of destruction, Contractor shall certify such destruction, in writing, to County upon written request. Contractor shall retain no copies of PHI and/or ePHI, except as provided below in paragraph (2) of this section.
   2) In the event that Contractor determines that returning or destroying the PHI and/or ePHI is not feasible, Contractor shall provide written notification to County of the conditions that make such return or destruction not feasible. Upon determination by Contractor that return or destruction of PHI and/or ePHI is not feasible, Contractor shall extend the protections of this Addendum to such PHI and/or ePHI and limit further uses and disclosures of such PHI and/or ePHI to those purposes which make the return or destruction not feasible, for so long as Contractor maintains such PHI and/or ePHI.

12. General Provisions.
   A. Retention Period. Whenever Contractor is required to document or maintain documentation pursuant to the terms of this Addendum, Contractor shall retain such documentation as prescribed by law.
   B. Amendment. The parties agree to take such action as is necessary to amend this Addendum from time to time as is necessary for County to comply with HITECH, the Privacy Rule, Security Rule, and HIPAA generally.
   C. Survival. The obligations of Contractor under Sections 3, 5, 6, 7, 8, 11.B and 12.A of this Addendum shall survive the termination or expiration of this Addendum.
   D. Regulatory and Statutory References. A reference in this Addendum to a section in HITECH, HIPAA, the Privacy Rule and/or Security Rule means the section(s) as in effect or as amended.
   E. Conflicts. The provisions of this Addendum shall prevail over any provisions in the Underlying Agreement that conflict or appear inconsistent with any provision in this Addendum.
   F. Interpretation of Addendum.
      1) This Addendum shall be construed to be part of the Underlying Agreement as one document. The purpose is to supplement the Underlying Agreement to include the requirements of the Privacy Rule, Security Rule, HIPAA and HITECH.
      2) Any ambiguity between this Addendum and the Underlying Agreement shall be resolved to permit compliance with the Privacy Rule, Security Rule, HIPAA and HITECH generally.
   G. Notices to County. All notifications required to be given by Contractor to County pursuant to the terms of this Addendum shall be made in writing (including via email) and delivered to the County to both of the addresses listed below by either registered or certified mail return receipt requested or guaranteed overnight mail with tracing capability, or at such other address as County may hereafter designate. All notices to County provided by Contractor pursuant to this Section shall be deemed given or made when received by County.

County HIPAA Privacy Officer: HIPAA Privacy Manager
County HIPAA Privacy Officer Address: 26520 Cactus Avenue, Moreno Valley, CA 92555
County HIPAA Privacy Officer Phone Number: (951) 486-4659

BY THE SIGNATURES BELOW THIS AGREEMENT IS AGREED AS OF THE EFFECTIVE DATE:

CROWDSTRIKE, INC.

By: Michelle Cline
Name: Michelle Cline
Title: Director, Legal
Date: 4/29/2025

COUNTY OF RIVERSIDE

By:
Name: V. MANUEL PEREZ
Title: CHAIR, BOARD OF SUPERVISORS
Date: JUN 10 2025

APPROVED AS TO FORM:
County Counsel

By: Esen Sainz
Esen Sainz
Deputy County Counsel
Date: 05/09/2025

ATTEST:
KIMBERLY A. RECTOR, Clerk

By _____
DEPUTY

JUN 10 2025 18.4

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. 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. **"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.
   g. **"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. 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.

b. 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").

c. 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.

5. Security Breach Response

In the event CrowdStrike discovers a Security Breach, CrowdStrike shall:

a. Without undue delay but no later than 72 hours of becoming aware, notify Customer of the discovery of the Security Breach. Such notice shall summarize the known circumstances of the Security Breach and the corrective action taken or to be taken by CrowdStrike.

b. Conduct an investigation of the circumstances of the Security Breach.

c. Use commercially reasonable efforts to remediate the Security Breach.

d. Use commercially reasonable efforts to communicate and cooperate with Customer concerning its response to the Security Breach.

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.

Copy of Legal Notices: Riverside University Health System

26520 Cactus Avenue

Moreno Valley, CA 92555

Attention: RUHS- IT Business & Legal

County HIPAA Privacy Officer: HIPAA Privacy Manager
County HIPAA Privacy Officer Address: 26520 Cactus Avenue, Moreno Valley, CA 92555

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
Dispute Resolution Outside North America
OMITTED

Exhibit C
Additional or Different Terms That May Apply to Certain Customers
RESERVED

CDW Healthcare

Riverside University Medical Center
QUOTE PLMK002
Crowdstrike 36 Month - Annual Pay

Quote Date:	May 28, 2025
Prepared By:	Tom Latzke
Phone:	(312) 705-0967
Email:	tomlat@cdw.com

Item	Description	Quantity	MSRP/Unit	Unit Price	Total Price
Quote Group 1 (Jun 13, 2025 - Jun 12, 2026) - Year 1					
CS.EPPENT.SOLN.T13.12M	Falcon Endpoint Protection	13,000	$29.36	$4.80	$62,400.00
CS.TG.STD.12M	Threat Graph Standard	12,300	$6.72	$1.50	$18,450.00
CS.PREVENT.SOLN.T13.12M	Prevent	13,000	$0.00	$0.00	$0.00
CS.INSIGHT.SOLN.T13.12M	Insight	13,000	$0.00	$0.00	$0.00
CS.AOW.SVC.T11.12M	Falcon Adversary OverWatch Endpoint	13,000	$23.65	$5.15	$66,950.00
CS.TG.STD.HPS.12M	Server Threat Graph Standard	700	$20.15	$4.43	$3,101.00
RR.HOS.ENT.ESTL.12M	Essential Support	1	$28,749.18	$18,519.04	$18,519.04
RR.PSO.ENT.NCAP.12M	University LMS Subscription New Customer Access Pass	20	$0.00	$0.00	$0.00
CS.FALCOMPU.SOLN.T9.12M	Falcon Complete Upgrade	11,700	$67.81	$10.59	$123,903.00
CS.FALCOMPONBC.SOLN.12M	Falcon Complete: Complimentary CID	1	$0.00	$0.00	$0.00
CS.ITPC.SOLN.T5.12M	Identity Threat Protection Complete Bundle	11,000	$69.89	$10.10	$111,100.00
CS.ITP.SOLN.T7.12M	Identity Threat Protection (Accounts)	11,000	$0.00	$0.00	$0.00
CS.ITPCU.SOLN.T5.12M	Identity Threat Protection Complete Upgrade (Accounts)	11,000	$0.00	$0.00	$0.00
CS.FCSS.SOLN.12M	Falcon Cloud Security Standalone	1	$0.00	$0.00	$0.00
CS.FCS.FLEX.RES.T1.12M	Falcon Cloud SecurityReserved - Flex - hourly average	10	$157.25	$35.99	$359.90
CS.CDR.SOLN.12M	Cloud Detection and Response	10	$0.00	$0.00	$0.00
CS.FALHORIZON.SOLN.12M	Falcon Horizon	10	$0.00	$0.00	$0.00
CS.TG.STD.HPS.12M	Server Threat Graph Standard	10	$20.15	$4.43	$44.30
CS.FCSCU.SOLN.12M	Falcon Cloud Security Complete Upgrade	10	$162.55	$36.70	$367.00
CS.AOWC.SVC.T1.12M	Falcon Adversary OverWatch Cloud	10	$68.00	$14.96	$149.60
CS.DEVICE.SOLN.T13.12M	Falcon Device Control	13,000	$3.47	$0.58	$7,540.00
CS.CHARLOTTEAI.SOLN.T11.12M	Charlotte AI	13,000	$10.00	$1.65	$21,450.00
CS.CHARLOTTEAI.EXP.SOLN.T1.12M	Charlotte AI Additional Usage (qty=350 queries/month)	1	$16,000.00	$15,666.16	$15,666.16
NR.PSO.NGS.OP1	NG-SIEM Operational Services-DOW Essentials	1	$90,000.00	$0.00	$0.00
CS.NGSIEMG.SOLN.T5.12M	Falcon Next-Gen SIEM Additional Ingestion (qty = GB)	100	$1,392.99	$0.00	$0.00
CS.NGSIEM180D.SOLN.12M	Falcon Next-Gen SIEM 180 Day Retention (qty = GB)	110	$155.50	$0.00	$0.00
CS.NGSIEMC.SOLN.T6.12M	Falcon Complete Next- Gen SIEM Upgrade (qty = GB)	110	$1,392.99	$0.00	$0.00
RR.HOS.ENT.ESTL.12M	Essential Support	1	$11,805.76	$0.00	$0.00
CS.FSR.180.SOLN.T11.12M	Falcon Search Retention - 180 days	13,000	$25.60	$0.00	$0.00
				Total:	$450,000.00

Item	Description	Quantity	MSRP/Unit	Unit Price	Total Price
Quote Group 2 (Jun 13, 2026 - Jun 12, 2027) Year 2					
CS.EPPENT.SOLN.T13.12M	Falcon Endpoint Protection	13,000	$29.36	$6.73	$87,490.00
CS.TG.STD.12M	Threat Graph Standard	12,300	$6.72	$1.57	$19,311.00
CS.PREVENT.SOLN.T13.12M	Prevent	13,000	$0.00	$0.00	$0.00
CS.INSIGHT.SOLN.T13.12M	Insight	13,000	$0.00	$0.00	$0.00
CS.AOW.SVC.T11.12M	Falcon Adversary OverWatch Endpoint	13,000	$23.65	$5.53	$71,890.00
CS.TG.STD.HPS.12M	Server Threat Graph Standard	700	$20.15	$4.72	$3,304.00
RR.HOS.ENT.ESTL.12M	Essential Support	1	$28,749.18	$27,651.77	$27,651.77
RR.PSO.ENT.NCAP.12M	University LMS Subscription New Customer Access Pass	20	$0.00	$0.00	$0.00
CS.FALCOMPU.SOLN.T9.12M	Falcon Complete Upgrade	11,700	$67.81	$17.62	$206,154.00
CS.FALCOMPONBC.SOLN.12M	Falcon Complete: Complimentary CID	1	$0.00	$0.00	$0.00
CS.ITPC.SOLN.T5.12M	Identity Threat Protection Complete Bundle	11,000	$69.89	$20.44	$224,840.00
CS.ITP.SOLN.T7.12M	Identity Threat Protection (Accounts)	11,000	$0.00	$0.00	$0.00
CS.ITPCU.SOLN.T5.12M	Identity Threat Protection Complete Upgrade (Accounts)	11,000	$0.00	$0.00	$0.00
CS.FCSS.SOLN.12M	Falcon Cloud Security Standalone	1	$0.00	$0.00	$0.00
CS.FCS.FLEX.RES.T1.12M	Falcon Cloud SecurityReserved - Flex - hourly average	10	$157.25	$45.99	$459.90
CS.CDR.SOLN.12M	Cloud Detection and Response	10	$0.00	$0.00	$0.00
CS.FALHORIZON.SOLN.12M	Falcon Horizon	10	$0.00	$0.00	$0.00
CS.TG.STD.HPS.12M	Server Threat Graph Standard	10	$20.15	$5.90	$59.00
CS.FCSCU.SOLN.12M	Falcon Cloud Security Complete Upgrade	10	$162.55	$47.55	$475.50
CS.AOWC.SVC.T1.12M	Falcon Adversary OverWatch Cloud	10	$68.00	$19.89	$198.90
CS.DEVICE.SOLN.T13.12M	Falcon Device Control	13,000	$3.47	$0.61	$7,930.00
CS.CHARLOTTEAI.SOLN.T11.12M	Charlotte AI	13,000	$10.00	$1.76	$22,880.00
CS.CHARLOTTEAI.EXP.SOLN.T1.12M	Charlotte AI Additional Usage (qty=350 queries/month)	1	$16,000.00	$16,672.49	$16,672.49
CS.NGSIEMG.SOLN.T5.12M	Falcon Next-Gen SIEM Additional Ingestion (qty = GB)	100	$1,392.99	$271.64	$27,164.00
CS.NGSIEM180D.SOLN.12M	Falcon Next-Gen SIEM 180 Day Retention (qty = GB)	110	$155.50	$30.33	$3,336.30
CS.NGSIEMC.SOLN.T6.12M	Falcon Complete Next- Gen SIEM Upgrade (qty = GB)	110	$1,392.99	$271.64	$29,880.40
RR.HOS.ENT.ESTL.12M	Essential Support	1	$11,805.76	$10,302.74	$10,302.74
CS.FSR.180.SOLN.T11.12M	Falcon Search Retention - 180 days	13,000	$25.60	$5.00	$65,000.00
				Total:	$825,000.00

Item	Description	Quantity	MSRP/Unit	Unit Price	Total Price
Quote Group 3 (Jun 13, 2027 - Jun 12, 2028) - Year 3					
CS.EPPENT.SOLN.T13.12M	Falcon Endpoint Protection	13,000	$29.36	$6.73	$87,490.00
CS.TG.STD.12M	Threat Graph Standard	12,300	$6.72	$1.57	$19,311.00
CS.PREVENT.SOLN.T13.12M	Prevent	13,000	$0.00	$0.00	$0.00
CS.INSIGHT.SOLN.T13.12M	Insight	13,000	$0.00	$0.00	$0.00
CS.AOW.SVC.T11.12M	Falcon Adversary OverWatch Endpoint	13,000	$23.65	$5.53	$71,890.00
CS.TG.STD.HPS.12M	Server Threat Graph Standard	700	$20.15	$4.72	$3,304.00
RR.HOS.ENT.ESTL.12M	Essential Support	1	$28,749.18	$27,651.77	$27,651.77
RR.PSO.ENT.NCAP.12M	University LMS Subscription New Customer Access Pass	20	$0.00	$0.00	$0.00
CS.FALCOMPU.SOLN.T9.12M	Falcon Complete Upgrade	11,700	$67.81	$17.62	$206,154.00
CS.FALCOMPONBC.SOLN.12M	Falcon Complete: Complimentary CID	1	$0.00	$0.00	$0.00
CS.ITPC.SOLN.T5.12M	Identity Threat Protection Complete Bundle	11,000	$69.89	$20.44	$224,840.00
CS.ITP.SOLN.T7.12M	Identity Threat Protection (Accounts)	11,000	$0.00	$0.00	$0.00
CS.ITPCU.SOLN.T5.12M	Identity Threat Protection Complete Upgrade (Accounts)	11,000	$0.00	$0.00	$0.00
CS.FCSS.SOLN.12M	Falcon Cloud Security Standalone	1	$0.00	$0.00	$0.00
CS.FCS.FLEX.RES.T1.12M	Falcon Cloud SecurityReserved - Flex - hourly average	10	$157.25	$45.99	$459.90
CS.CDR.SOLN.12M	Cloud Detection and Response	10	$0.00	$0.00	$0.00
CS.FALHORIZON.SOLN.12M	Falcon Horizon	10	$0.00	$0.00	$0.00
CS.TG.STD.HPS.12M	Server Threat Graph Standard	10	$20.15	$5.90	$59.00
CS.FCSCU.SOLN.12M	Falcon Cloud Security Complete Upgrade	10	$162.55	$47.55	$475.50
CS.AOWC.SVC.T1.12M	Falcon Adversary OverWatch Cloud	10	$68.00	$19.89	$198.90
CS.DEVICE.SOLN.T13.12M	Falcon Device Control	13,000	$3.47	$0.61	$7,930.00
CS.CHARLOTTEAI.SOLN.T11.12M	Charlotte AI	13,000	$10.00	$1.76	$22,880.00
CS.CHARLOTTEAI.EXP.SOLN.T1.12M	Charlotte AI Additional Usage (qty=350 queries/month)	1	$16,000.00	$16,672.49	$16,672.49
CS.NGSIEMG.SOLN.T5.12M	Falcon Next-Gen SIEM Additional Ingestion (qty = GB)	100	$1,392.99	$271.64	$27,164.00
CS.NGSIEM180D.SOLN.12M	Falcon Next-Gen SIEM 180 Day Retention (qty = GB)	110	$155.50	$30.33	$3,336.30
CS.NGSIEMC.SOLN.T6.12M	Falcon Complete Next- Gen SIEM Upgrade (qty = GB)	110	$1,392.99	$271.64	$29,880.40
RR.HOS.ENT.ESTL.12M	Essential Support	1	$11,805.76	$10,302.74	$10,302.74
CS.FSR.180.SOLN.T11.12M	Falcon Search Retention - 180 days	13,000	$25.60	$5.00	$65,000.00
				Total:	$825,000.00
Group 6 (May 30, 2025 - May 29, 2028) - Total Payment					

Grand total	$2,100,000.00

Terms: quotes are good for 45 days
Prices may change at anytime
Please contact your account manager for questions

CROWDSTRIKE, INC., a Delware corporation

By: DocuSigned by: Benny Huang 942AFFBE9616405...
Name: Benny Huang
Title: VP, Revenue Controller
Date: 4/29/2025

DS SG

COUNTY OF RIVERSIDE, a political subdivision of the state of California, on behalf of its Riverside University Health System Medical Center

By: V. MANUEL PEREZ
Name:
Title: Board of Supervisors, Chair
Date: JUN 10 2025

ATTEST: Kimberly Rector
Clerk of the Board
By:
Deputy

APPROVED TO FORM:
County Counsel
By: Esen Sainz
Name: Esen Sainz
Title: Deputy County Counsel
Date: 05/09/2025

Send notices to:

150 Mathilda Place, 3rd Floor
Sunnyvale, CA 94086
With a copy to: legal@crowdstrike.com

Notice Address:
Riverside University Health System- Medical Center
Address: 26520 Cactus Avenue
City: Moreno Valley State: CA Zip: 92555
Attn:
Country:

JUN 10 2025 18.4

CROWDSTRIKE MASTER AGREEMENT

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 County of Riverside, a political subdivision of the state of California on behalf of its Riverside University Health System Medical Center ("**Customer**") are entered into as of the date signed by the last party (the "**Effective Date**").

These CrowdStrike Terms and Conditions 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.

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).

"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

JUN 10 2025 18.4

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 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 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 including Section 13 below, 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.

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) employ 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.

5.1 Fees. Professional Services will commence on a mutually agreed upon date. Estimates provided for Professional Services performed on a time-and-material basis are estimates only and not a guaranteed time of completion. Professional Services performed on a fixed fee basis are limited to the scope of services stated in the applicable Order.

5.2 Ownership of Deliverables. Professional Services do not constitute "works for hire," "works made in the course of duty," or similar terms under laws where the transfer of intellectual property occurs on the performance of services to a payor. The only deliverable arising from the Professional Services is a report consisting primarily of CrowdStrike's findings, recommendations, and adversary information. Customer owns the copy of the report (including without limitation, all of Customer's Confidential Information therein) delivered to Customer ("**Deliverable**"), subject to CrowdStrike's ownership of the CrowdStrike Materials. Customer agrees that relative to Customer, CrowdStrike exclusively owns any and all software (including object and source code), flow charts, algorithms, documentation, adversary information, report templates, know-how, inventions, techniques, models, CrowdStrike trademarks, ideas and any and all other works and materials developed by CrowdStrike in connection with performing the Professional Services (including without limitation all intellectual property rights therein and thereto) (collectively, the "**CrowdStrike Materials**") and that title shall remain with CrowdStrike. For the avoidance of doubt, the CrowdStrike Materials do not include any Customer Confidential Information or other Customer provided materials or data. Upon payment in full of the amounts due hereunder for the applicable Professional Services and to the extent the CrowdStrike Materials are incorporated into the Deliverable(s), Customer shall have a perpetual, non-transferable (except as expressly provided in the Section entitled *Assignment*), non-exclusive license to use the CrowdStrike Materials solely as a part of the Deliverable(s) for Customer's Internal Use.

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 or 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. 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; or (iv) rightfully obtained by Recipient from third parties without an obligation of confidentiality.

7.2 Restrictions on Use. Except as allowed in Section .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. If the

Recipient is legally required to disclose the Discloser's Confidential Information as part of: (x) a legal proceeding to which the Discloser is a party but the Recipient is not; or (y) a government or regulatory investigation of the Discloser, the Discloser shall pay all of the Recipient's reasonable and actual out of pocket legal fees and expenses (as evidenced by reasonably detailed invoices) and will reimburse the Recipient for its reasonable costs and fees of compiling and providing such Confidential Information, including, a reasonable hourly rate for time spent preparing for, and participating in, depositions and other testimony.

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 California Public Records Act and Brown Act. CrowdStrike acknowledges that Customer is a governmental entity subject to the public records and meeting laws of the State of California, including the California Public Records Act (Government Code Section 6250 et seq.) and the California Brown Act (Government Code Section 54590 et seq.). Notwithstanding any other provision contained in this Agreement, any information (including Confidential Information), communications, and documents given by CrowdStrike to Customer and meetings involving Customer may be subject to disclosure pursuant to the Public Records Act and Brown Act. To the extent Customer is required by law to disclose any of the above-described information, communications, and documents, Customer shall comply with such law; provided, however, to the extent legally permitted Customer shall (a) give CrowdStrike prompt written notice of such requirement or request prior to such disclosure; and (b) a reasonable opportunity to review and comment upon the disclosure and request confidential treatment or a protective order pertaining thereto prior to Customer making such disclosure, so long as such opportunities described in this Section 7.5(b) do not prevent Customer from complying with the laws in this Section 7.5.

7.6 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.

8.7 Additional Terms That May Apply. See Exhibit C for additional warranties that may apply to certain Customers.

9. Indemnification.

9.1 CrowdStrike's Obligation. CrowdStrike shall at its cost and expense: (i) defend and/or settle any claim brought against Customer, its directors, officers, and employees by an unaffiliated third party alleging (a) that an Offering infringes or violates that third party's intellectual property rights, or (b) personal injury or death and/or damage to, or loss or destruction of, an real or tangible personal property to the extent caused by CrowdStrike's negligence or intentional misconduct, 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: (x) gives CrowdStrike prompt written notice of such claim; (y) 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 (z) 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.

9.2 Indemnity for Breach of Business Associate Agreement. CrowdStrike shall at its cost and expense: (i) defend and/or settle any claim brought against Customer, its directors, officers, and employees by an unaffiliated third party alleging CrowdStrike's breach of its obligations under the Business Associate Agreement executed by and between the parties which results in the compromise of Customer Personal Health Information, 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. **CrowdStrike and Customer each acknowledge and agree such liability in this Section 9.2 shall not exceed two million five-hundred thousand dollars ($2,500,000) (the "Specified Damages Cap").**

9.3 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.

9.4 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.

9.5 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 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.

10.2 Additional or Different Terms That May Apply. See Exhibit C for additional or different terms related to liability that may apply to certain Customers.

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 3.3 (*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. Should Customer terminate this Agreement for CrowdStrike's uncured, material breach, CrowdStrike will refund the prepaid fee prorated for the unused period of the applicable Subscription/Order Term. 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, 3.3, 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.

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. Except as otherwise provided in Exhibit B (if applicable), 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 California, 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 Riverside County, California, 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 Disputes: The parties shall attempt to resolve any disputes amicably at the working level. If that is not successful, the dispute shall be referred to the senior management of the parties. CrowdStrike shall proceed diligently with the performance of this Agreement pending the resolution of a dispute. This Section 14.8 (Disputes) will not prohibit either CrowdStrike or Customer from seeking preliminary or injunctive relief or from exercising any other rights under this Agreement, including without limitation any right to suspend access to the Offerings or terminate this Agreement under Section 13 (Suspension and Termination).

14.9 Signatures. This Agreement and any Orders, as applicable, may be executed in any number of counterparts, each of which will be an original, but all of which together will constitute one instrument. Each party of this Agreement agrees to the use of electronic signatures, such as digital signatures which substantially conform to the requirements of the California Uniform Electronic Transactions Act (("CUETA") Cal. Civ. Code §§ 1633.1 to 1633.17), for executing this Agreement. The parties further agree that the electronic signatures of the parties included in this Agreement are intended to authenticate this writing and to have the same force and effect as manual signatures. Electronic signature means an electronic sound, symbol, or process attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign the electronic record. The CUETA authorizes use of an electronic signature for transactions and contracts among parties in California, including a government agency. Digital signature means an electronic identifier, created by computer, intended by the party using it to have the same force and effect as the use of a manual signature, and shall be reasonably relied upon by the parties. For purposes of this section, a digital signature is a type of "electronic signature" as defined in subdivision (i) of Section 1633.2 of the Civil Code.

15. INSURANCE. CROWDSTRIKE shall procure and maintain or cause to be maintained, at its sole cost and expense, the following insurance coverage's during the term of this Agreement. As respects to the insurance section only, the CUSTOMER herein refers to the County of Riverside, its Agencies, Districts, Special Districts, and Departments, their respective directors, officers, Board of Supervisors, employees, elected or appointed officials, agents or representatives as Additional Insureds.

A. Workers' Compensation: If CROWDSTRIKE has employees as defined by the State of California, the CROWDSTRIKE shall maintain statutory Workers' Compensation Insurance (Coverage A) as prescribed by the laws of the State of California. Policy shall include Employers' Liability (Coverage B) including Occupational Disease with limits not less than $1,000,000 per person per accident.

B. Commercial General Liability: Commercial General Liability insurance coverage, including but not limited to, premises liability, products and completed operations liability, personal and advertising injury covering claims which may arise from or out of CROWDSTRIKE'S performance of its obligations hereunder. Policy shall name the CUSTOMER as Additional Insured via blanket endorsement. Policy's limit of liability shall not be less than $2,000,000 per occurrence combined single limit.

C. Vehicle Liability: If vehicles or mobile equipment are used in the performance of the obligations under this Agreement, then CROWDSTRIKE shall maintain liability insurance for all owned, non-owned or hired vehicles so used in an amount not less than $1,000,000 per occurrence combined single limit.

E. Cyber Liability Insurance, with limits not less than $2,000,000 per occurrence or claim, $2,000,000 aggregate. Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by CrowdStrike in this agreement and shall include, claims involving infringement of intellectual property, including trademark, trade dress, invasion of privacy violations, information theft, damage to or destruction of electronic in-formation, release of private information, alteration of electronic information, extortion and network security. The policy shall provide coverage for breach response costs as well as regulatory fines and penalties as well as credit monitoring expenses with limits sufficient to respond to these obligations.

G. General Insurance Provisions - All lines:

1) Any insurance carrier providing insurance coverage hereunder shall have an A M BEST rating of not less than A: VIII (A:8)

2) CROWDSTRIKE or an authorized representative shall furnish the CUSTOMER of Riverside with a Certificate(s) of Insurance and blanket endorsement(s). Further, said Certificate(s) of insurance shall contain the covenant that a minimum of thirty (30) days written notice shall be given to the County of Riverside of any material modification, cancellation, expiration or reduction in coverage of such insurance.

3) CROWDSTRIKE shall pass down the insurance obligations contained herein to all tiers of subcontractors working under this Agreement.

4) The insurance requirements contained in this Agreement may be met with a program(s) of self-insurance.