DATA PRIVACY AGREEMENT

INCLUDING
PARENTS BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY
AND
SUPPLEMENTAL INFORMATION ABOUT THE
Agreement

1. Purpose

(a) This Data Privacy Agreement (DPA or DPA Agreement) supplements the CrowdStrike Terms and Conditions (Vendor AGREEMENT) between Capital Region BOCES (BOCES) and CrowdStrike, Inc. (Vendor), to ensure that the Vendor AGREEMENT conforms to the requirements of New York State Education Law Section 2-d and any implementing Regulations of the Commissioner of Education (collectively referred to as "Section 2-d"). This Agreement consists of the terms of this DPA Agreement, a copy of BOCES Parents Bill of Rights for Data Security and Privacy signed by Vendor and attached hereto, and the Supplemental Information document signed by Vendor and attached hereto.

(b) To the extent that any terms contained within the Vendor AGREEMENT, or any terms contained within any other agreements attached to and made a part of the Vendor AGREEMENT, conflict with the terms of this DPA, the terms of this DPA will prevail to the extent of such conflict. In the event that Vendor has online or written Terms of Service ("TOS") that would otherwise be applicable to its customers or users of its products or services that is the subject of the Vendor AGREEMENT, to the extent that any term of the TOS conflicts with the terms of this DPA, the terms of this DPA will prevail to the extent of such conflict.

2. Definitions

Any capitalized term used within this DPA that is also found in the Vendor AGREEMENT will have the same definition as contained within this DPA.

In addition, as used in this Exhibit:

(a) "Student Data" means personally identifiable information, as defined in Section 2-d, from student records that Vendor receives from a Participating Educational Agency pursuant to Vendor AGREEMENT.

(b) "Teacher or Principal Data" means personally identifiable information relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of New York Education Law Sections 3012-c or 3012-d, that Vendor receives from a Participating Educational Agency pursuant to the Vendor AGREEMENT.

(c) "Protected Data" means Student Data and/or Teacher or Principal Data to the extent

collected by Vendor and processed in Vendor's computer systems hosting the 'Falcon EPP Platform'.

(d) "Participating Educational Agency" means a school district within New York State that purchases certain shared instructional technology services and software through a Cooperative Educational Services Agreement with BOCES, and as a result is licensed to use Vendor's Product pursuant to the terms of the Vendor AGREEMENT.

3. Confidentiality of Protected Data

(a) Vendor acknowledges that the Protected Data it receives pursuant to the Vendor AGREEMENT may originate from several Participating Educational Agencies located across New York State, and that this Protected Data belongs to and is owned by the Participating Educational Agency from which it originates.

(b) Vendor will maintain the confidentiality of the Protected Data it receives in accordance with federal and state law (including but not limited to Section 2-d) to the extent such laws, by their terms, are directly applicable to Vendor in performance of the services and provision of the products under the Vendor AGREEMENT.

(c) BOCES hereby agrees to use best efforts not to give or provide CROWDSTRIKE with access to any Protected Data, including without limitation educational records subject to FERPA.

4. Data Security and Privacy Plan

Vendor agrees that it will protect the confidentiality, privacy and security of the Protected Data received from Participating Educational Agencies in accordance with the BOCES Parents Bill of Rights for Data Privacy and Security, a copy of which has been signed by Vendor and is set forth below.

Additional elements of Vendor' Data Security and Privacy Plan are as follows:

(a) In order to comply with all state, federal, and local data security and privacy requirements, including those contained within this DPA, in each case, to the extent directly applicable to Vendor in performance of the services and provision of the products under the Vendor AGREEMENT, Vendor will maintain appropriate technical and organizational safeguards commensurate with the sensitivity of the Protected Data processed by Vendor, which are designed to protect the security, confidentiality, and integrity of such Protected Data and protect such Protected 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 Vendor Systems").

(b) In order to protect the security, confidentiality and integrity of the Protected Data that it receives under the Vendor AGREEMENT, Vendor will have the following reasonable administrative, technical, operational and physical safeguards and practices in place throughout the term of the Vendor AGREEMENT: the Information Security Controls for Vendor Systems (as defined

above).

(c) Vendor will comply with all obligations set forth in BOCES "Supplemental Information about the AGREEMENT" a copy of which has been signed by Vendor and is set forth below.

(d) For any of its officers or employees (or officers or employees of any of its assignees) who have access to Protected Data, Vendor has provided or will provide training on the federal and state laws, which laws are, by their terms, directly applicable to Vendor in performance of the services and provision of the products under the Vendor AGREEMENT and which govern confidentiality of such data prior to their receiving access.

(e) In the event that Vendor engages any subcontractors, assignees, or other authorized agents to perform its obligations under the Vendor AGREEMENT, it will require such subcontractors, assignees, or other authorized agents to execute written agreements as more fully described in BOCES "Supplemental Information about the Vendor AGREEMENT," below. For purposes of this DPA and the Supplemental Information about the AGREEMENT attached hereto, "subcontractors" shall mean any person or entity that has been retained by Vendor to perform all or a portion of professional services under the Vendor AGREEMENT directly and uniquely to BOCES or a Participating Educational Agency.

(f) Vendor will manage data security and privacy incidents that implicate Protected Data, including identify breaches and unauthorized disclosures of Protected Data, and Vendor will provide prompt notification of any breaches or unauthorized disclosures of Protected Data in accordance with Section 6 of this Data Sharing and Confidentiality Agreement.

(g) Vendor will implement procedures for the return, transition, deletion and/or destruction of Protected Data at such time that the AGREEMENT is terminated or expires, as more fully described in BOCES "Supplemental Information about the AGREEMENT," below.

5. Additional Statutory and Regulatory Obligations

Vendor acknowledges that it has the following additional obligations with respect to any Protected Data received from Participating Educational Agencies, and that any failure to fulfill one or more of these statutory or regulatory obligations shall be a breach of the Vendor AGREEMENT and the terms of this Data Privacy Agreement:

(a) To the extent that FERPA is, by its terms, applicable to Vendor's delivery of products and services under the Vendor AGREEMENT and imposes obligations directly upon Vendor in its role as an information technology services provider with respect to such products and services, Vendor shall limit internal access to education records to those individuals that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA).

(b) Limit internal access to Protected Data to only those employees or subcontractors that need access in order to assist Vendor in fulfilling one or more of its obligations under the Vendor

AGREEMENT.

(c) Not use education records for any purposes other than those explicitly authorized in this Data Sharing and Confidentiality Agreement and in the Vendor AGREEMENT.

(d) Not disclose any personally identifiable information to any other party, except for authorized representatives of Vendor using the information to carry out Vendor's obligations under the Vendor AGREEMENT, unless:

(i) the parent or eligible student has provided prior written consent; or

(ii) the disclosure is required by statute or court order and notice of the disclosure is provided to Participating Educational Agency no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order.

(e) Maintain reasonable administrative, technical, and physical safeguards designed to protect the security, confidentiality, and integrity of personally identifiable student information in its custody;

(f) Use encryption technology that complies with Section 2-d, as more fully set forth in BOCES "Supplemental Information about the Vendor AGREEMENT," below.

(g) Provide notification to BOCES (and Participating Educational Agencies, to the extent required by, and in accordance with, Section 6 of this Data Privacy Agreement) of any breach of security resulting in an unauthorized release of Protected Data by Vendor or its assignees or subcontractors in violation of state or federal law or other obligations relating to data privacy and security contained herein.

(h) Subject to the Section entitled *Limitation of Liability* in the Vendor AGREEMENT, promptly reimburse BOCES, another BOCES, or a Participating School District for the full cost of notification, in the event they are required under Section 2-d to notify affected parents, students, teachers or principals of a breach or unauthorized release of Protected Data attributed to Vendor or its subcontractors orassignees.

6. Notification of Breach and Unauthorized Release

(a) Vendor shall promptly notify BOCES of any breach or unauthorized release of Protected Data in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after Vendor has discovered or been informed of the breach or unauthorized release.

(b) Vendor will provide such notification to BOCES by contacting the BOCES Data Protection Officer, at dpo@neric.org.

(c) Vendor will provide reasonable cooperation to BOCES and provide as much information as reasonably possible directly to the Data Protection Officer (DPO) or designee about the incident, including but not limited to and to the extent practicable: a description of the incident, the

date of the incident, the date Vendor discovered or was informed of the incident, a description of the types of personally identifiable information involved, an estimate of the number of records affected, the Participating Educational Agencies affected, what the Vendor has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of Protected Data, and contact information for Vendor representatives who can assist affected individuals that may have additional questions.

(d) Vendor acknowledges that upon initial notification from Vendor, BOCES, as the educational agency with which Vendor contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department ("CPO"). Vendor shall not provide any notification to the CPO directly that identifies Capital Region BOCES in connection with such incident. In the event the CPO contacts Vendor directly or requests more information from Vendor regarding the incident after having been initially informed of the incident by BOCES, Vendor will promptly inform the Data Protection Officer or designees.

(e) Vendor will consult directly with the Data Protection Officer or designees prior to providing any further notice of the incident (written or otherwise) that identifies Capital Region BOCES in connection with such incident, directly to any other BOCES or Regional Information Center, or any affected Participating Educational Agency.

BY Vendor:

Mike Forman

7A8C240C3686CBF02985F43A5EC3AD85 contractworks.

Signature

VP/Controller

Title

02/02/21

Date

Appendix 1
Information Security Controls for Vendor 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 Vendor'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 Vendor 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 Vendor Systems and the organization's premises b. Maintain controls designed to limit access to Personal Data, relevant Vendor Systems and the facilities hosting the Vendor Systems to authorized personnel c. Review personnel access rights on a regular and periodic basis d. Maintain physical access controls to facilities containing Vendor Systems, including by using access cards or fobs issued to Vendor personnel as appropriate e. Maintain policies requiring termination of physical and electronic access to Personal Data and Vendor Systems after termination of an employee f. Implement access controls designed to authenticate users and limit access to Vendor Systems g. Implement policies restricting access to the data center facilities hosting Vendor Systems to approved data center personnel and limited and approved Vendor personnel h. Maintain dual layer access authentication processes for Vendor employees with administrative access rights to Vendor 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 Vendor 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 Vendor 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

PARENTS' BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY

Albany-Schoharie-Schenectady-Saratoga BOCES (BOCES) is committed to protecting the privacy and security of personally identifiable information about students who attend BOCES instructional programs in accordance with applicable law, including New York State Education Law Section 2-d.

To further these goals, BOCES wishes to inform parents of the following:

(1) A student's personally identifiable information cannot be sold or released for any commercial purposes.

(2) Parents have the right to inspect and review the complete contents of their child's education record, including any student data maintained by the Capital Region BOCES. This right of inspection of records is consistent with the federal Family Educational Rights and Privacy Act (FERPA). Under the more recently adopted regulations (Education Law §2-d), the rights of inspection are extended to include data, meaning parents have the right to inspect or receive copies of any data in their child's educational record. The New York State Education Department (SED) will develop further policies and procedures related to these rights in the future.

Requests to inspect and review a child's education record should be directed to: Data Protection Officer, dpo@neric.org, 900 Watervliet-Shaker Road, Albany, NY 12205.

(3) State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.

(4) A complete list of all student data elements collected by the State is available for public review at http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx, or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

(5) Parents have the right to have complaints about possible breaches of student data addressed. Complaints may be directed to the NYS Chief Privacy Officer by writing to the New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be directed to the Chief Privacy Officer via email at: CPO@mail.nysed.gov.

BY Vendor:

Mike Forman

7A8C240C3686CBF82985F43A5EC3AD85 contractworks

Signature

VP/Controller

Title

02/02/2021

Date

SUPPLEMENTAL INFORMATION

ABOUT THE AGREEMENT BETWEEN
Albany-Schoharie-Schenectady-
Saratoga BOCES AND Vendor

BOCES has entered into an Agreement ("AGREEMENT") with Vendor ("Vendor"), which governs the availability to Participating Educational Agencies of the following Product(s): Vendor's cloud-based software or other products, including without limitation: Falcon Prevent (Next-Generation Antivirus); Falcon Insight (Endpoint Detection & Response); Falcon Discover (IT Hygiene); Falcon Firewall Management (Firewall Management and Policy Enforcement); Device Control (USB Monitoring and Policy Enforcement); Falcon Spotlight (Vulnerability Assessment); Falcon Forensics; Falcon X (Threat Intelligence); Falcon X Premium (Threat Intelligence). Vendor's product-related services, including without limitation: Falcon OverWatch; Falcon Complete Team; technical support services for certain products provided by Vendor; training; and any other Vendor services provided or sold with products. Vendor's professional services, including without limitation incident response, investigation and forensic services related to cyber-security adversaries, tabletop exercises, and next generation penetration tests related to cyber-security.

Pursuant to the AGREEMENT, Participating Educational Agencies may provide to Vendor, and Vendor may receive, personally identifiable information about students, or teachers and principals, that is protected by Section 2-d of the New York State Education Law ("Protected Data").

Exclusive Purpose for which Protected Data will be Used:

The exclusive purpose for which Vendor is being provided access to Protected Data is to provide Participating Educational Agencies with the functionality of the product(s), product-related services, and/or professional services listed above.

Vendor agrees that it will not use the Protected Data for any other purposes not explicitly authorized in the AGREEMENT. Protected Data received by Vendor, or any of Vendor's subcontractors, assignees, or other authorized agents, will not be sold, or released or used for any commercial or marketing purposes.

Oversight of Subcontractors: In the event that Vendor engages subcontractors, assignees, or other authorized agents to perform one or more of its obligations under the AGREEMENT (including any hosting service provider), it will require those to whom it discloses Protected Data to execute legally binding agreements acknowledging such subcontractors, assignees, or other authorized agent's obligation to comply with the same data security and privacy standards required of Vendor under the AGREEMENT and applicable state and federal law. Vendor will ensure that Vendor has agreements in place with such subcontractors, assignees, or other authorized agents that allow Vendor to meets its obligations hereunder.

Duration of AGREEMENT and Protected Data Upon Expiration:

- The AGREEMENT commences on the Effective Date (as defined in the AGREEMENT) and expires or terminates in accordance with the terms thereof. Upon expiration of the AGREEMENT without renewal, or upon termination of the AGREEMENT prior to expiration, Vendor will securely delete or otherwise destroy any and all Protected Data remaining in the possession of Vendor or its assignees or subcontractors within 90 days of such expiration or termination. If requested by a Participating Educational Agency, Vendor will assist that entity in exporting all Protected Data hosted by Vendor at the time of such request , prior todeletion.

- During the applicable subscription/order term, at BOCES request, Vendor will make available to BOCES Protected Data being hosted by Vendor at the time of such request.
- Vendor agrees that unless otherwise required by applicable law, neither it nor its subcontractors, assignees, or other authorized agents will retain any copy or summary or extract of the Protected Data, on any storage medium whatsoever. Upon request, Vendor and/or its subcontractors, assignees, or other authorized agents will provide a certification from an appropriate officer that these requirements have been satisfied in full.

Challenging Accuracy of Protected Data: Parents or eligible students can challenge the accuracy of any Protected Data provided by a Participating Educational Agency to Vendor, by contacting the student's district of residence regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers or principals may be able to challenge the accuracy of APPR data provided to Vendor by following the appeal process in their employing school district's applicable APPR Plan.

Data Storage and Security Protections: Any Protected Data Vendor receives will be hosted on systems maintained by Vendor or third parties engaged by Vendor, in a secure data center facility. The measures that Vendor will take to protect Protected Data include adoption of technologies, safeguards and practices that align with the NIST Cybersecurity Framework (i.e., NIST SP 800-53) and industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.

Encryption of Protected Data: Vendor (or, if applicable, its subcontractors) will protect Protected Data in its custody from unauthorized disclosure while in motion or at rest, using a minimum of AES/128 bit ciphers.

BY Vendor:

Mike Forman

7A8C240C3686CBF02985F43A5EC3AD85 contractworks

Signature

VP/Controller

Title

02/02/2021

Date