

## 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 meet 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 to deletion.

- 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  
 Signature 7A8C240C3686CBF02985F43A5EC3AD85 contractworks.

VP/Controller

**Title**

02/02/2021

**Date**