https://www.btboces.org/Downloads/Parents%20Bill%20of%20Rights%20edit.pdf

This section to be completed by the Third-Party Contractor and returned to Broome-Tioga BOCES

Section 1: Does the Third-Party Contractor have access to student data and/or teacher or principal data as those terms are defined by law?

☒ Yes
Please complete Sections 2, 3 and 4

☐ No
Please complete Section 3

Section 2: Supplemental Information Details
Third-Party Contractors subject to New York Education Law § 2-d – please complete the table below

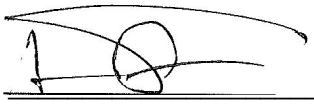
SUPPLEMENTAL INFORMATION ELEMENT	SUPPLEMENTAL INFORMATION
Please list the exclusive purpose(s) for which the student data or teacher or principal data will be used by the third-party contractor, as defined in the contract (or list the section(s) in the contract where this information can be found)	Section 4- How we use your information www.checkpoint.com/privacy/
Please list how the contractor will ensure that any other entities with which it shares the protected data, if any, will comply with the data protection and security provisions of law, regulation and this contract (or list the section(s) in the contract where this information can be found)	Section 5- Disclosure of your information to third parties www.checkpoint.com/privacy/
Please list when the agreement expires and what happens to the protected data when the agreement expires (or list the section(s) in the contract where this information can be found)	Section 8- How long we keep your personal data www.checkpoint.com/privacy/
Please list how a parent, student, or eligible student may challenge the accuracy of the protected data that is collected; if they can challenge the accuracy of the data, describe how (or list the section(s) in the contract where this information can be found)	Section 9- Your rights + Section 11 www.checkpoint.com/privacy/
Please list where the protected data will be stored (described in a way that protects data security), and the security protections taken to ensure such data will be protected and data security and privacy risks mitigated (or list the section(s) in the contract where this information can be found)	Section 7- How we safeguard your information www.checkpoint.com/privacy/
Please list how the data will be protected using encryption (or list the section(s) in the contract where this information can be found)	Section 7- Protection of personal information https://research.checkpoint.com/privacy-policy/

Section 3: Agreement and Signature

By signing below, you agree:

- The information provided in this document by the Third-Party Contractor is accurate
- To comply with the terms of Broome-Tioga BOCES Parents' Bill of Rights for Data Privacy and Security (applicable to Third-Party Contractors subject to New York Education Law § 2-d only)

Company Name Check Point Software Technologies Product Name Harmony Endpoint (formally Sandblast Agent).

Printed Name John Slavitt Signature  Date 7/29/21

Section 4: Data Privacy Rider for All Contracts Involving Protected Data Pursuant to New York State Education Law §2-C and §2-D

BOCES and the Third-Party Contractor agree as follows:

1. Definitions:
    a. Protected Information means personally identifiable information of students from student education records as defined by FERPA, as well as teacher and Principal data regarding annual professional performance reviews made confidential under New York Education Law §3012-c and §3012-d;
    b. Personally Identifiable Information (PII) means the same as defined by the regulations implementing FERPA (20 USC §1232-g);

2. Confidentiality of all Protected Information shall be maintained in accordance with State and Federal Law and the BOCES's Data Security and Privacy Policy;

3. The Parties agree that the BOCES's Parents' Bill of Rights for Data Security and Privacy are incorporated as part of this agreement, and the Third-Party Contractor shall comply with its terms;

4. The Third-Party Contractor agrees to comply with New York State Education Law §2-d and its implementing regulations;

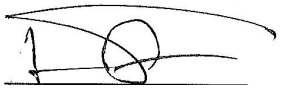
5. The Third-Party Contractor agrees that any officers or employees of the Third-Party Contractor, and its assignees who have access to Protected Information, have received or will receive training on Federal and State law governing confidentiality of such information prior to receiving access;

6. The Third-Party Contractor shall:
    a. limit internal access to education records to those individuals that are determined to have legitimate educational interests;
    b. not use the education records for any other purposes than those explicitly authorized in its contract or written agreement. Unauthorized use specifically includes, but is not limited to, selling or disclosing personally identifiable information for marketing or commercial purposes or permitting, facilitating, or disclosing such information to another Third-Party for marketing or commercial purposes;
    c. except for authorized representatives of the Third-Party Contractor to the extent they are carrying out the contract or written agreement, not disclose any personally identifiable information to any other party;
        i. without the prior written consent of the parent or eligible student; or
        ii. unless required by statute or court order and the party provides notice of the disclosure to the New York State Education Department, Board of Education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by statute or court order;
    d. maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in its custody;
    e. use encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the Secretary of the United States Department of Health and Human Services in guidance issued under Section 13402(H)(2) of Public Law §111-5;
    f. adopt technology, safeguards and practices that align with the NIST Cybersecurity Framework;
    g. impose all the terms of this rider in writing where the Third-Party Contractor engages a subcontractor or other party to perform any of its contractual obligations which provides access to Protected Information.

Agreement and Signature

By signing below, you agree to the Terms and Conditions in this Rider:

Company Name Check Point Software Technlogies Product Name Harmony Endpoint (formally Sandblast Agent).

Printed Name John Slavitt Signature  Date 7/29/21

Cookies Notice (/privacy/cookies/) | Website Terms and Conditions (/privacy/terms/)

Privacy Policy

Check Point Software Technologies Ltd, including all of its affiliates (including subsidiaries) worldwide (collectively, “Check Point,” “we,” “us,” or “our”) value the privacy of individuals who use or express interest in the Check Point Websites (as defined below), and the Check Point products and services (collectively, our “Services”). This privacy policy (the “Privacy Policy”) explains how we collect, use, and disclose Personal Data and applies to all of Check Point’s Services.

1. GENERAL INFORMATION

1.1 “Personal Data” means any data which relates to a living individual who can be identified from that data or from that data and other information which is in the possession of, or is likely to come into the possession of, Check Point (or its representatives or service providers). In addition to factual information, it includes any expression of opinion about an individual and any indication of the intentions of Check Point or any other person in respect of an individual.

1.2 Beyond this Privacy Policy, your use of our Services is also subject to applicable End-user License Agreement available at our website.

1.3 If you are a California resident, our California Resident Privacy Notice (/privacy/ccpa-notice/) provides more information about your California privacy rights and explains how you can exercise those rights.

1.4. If you are using the Check Point ZoneAlarm services and products, please refer to our ZoneAlarm Privacy Policy (https://www.zonealarm.com/privacy).

2. THE SOURCES OF THE INFORMATION WE COLLECT

This Privacy Policy concerns the following sources of information that we collect in connection with our Service, which include:

Our websites (e.g. www.checkpoint.com) ("Check Point Websites"), emails, marketing communication;

Information we received through our business partners and vendors; and

Information we receive through and from all of our Services (as defined above).

3. THE TYPES OF PERSONAL DATA WE COLLECT

We may collect and receive a variety of information from you or about you or your devices from various sources, as described below. If you do not provide your Personal Data when requested, you may not be able to use our Services if that information is necessary to provide you with our Services or if we are legally required to collect it.

3.1 **Information that you provide to Check Point.** This includes Personal Data about you that you provide to us. The nature of the Services you are requesting or using will determine the kind of Personal Data we might ask for, though such information may include (by way of a non-exhaustive list):

basic Personal Data (such as first name; family name; position in the company [title]; company name; company email address; business phone number; business address; city; postcode; country);

any information that you choose to share through our Services which may be considered Personal Data. (Please note that Check Point does not collate information included on Check Point internet forums together with Personal Data from your User Center account or profile);

3.2 **Information that we collect or generate about you.** This includes (by way of non-exhaustive list):

File with your contact history to be used for enquiry purposes so that we may ensure that you are satisfied with our Services;

Through our cloud security services, traffic and security reports that include information on the internet usage of the organization's computer users (e.g. what websites were visited by each user, any documents downloaded, security incidents, prevention measures taken by the gateway, etc.);

Activity data relating to the use of protected documents, such as altering a document's permissions and information regarding the individual that performed the activity;

Information about you provided from third parties' sources; and

Through our cloud Harmony Email & Office service, the files and email correspondence (included the content therein) found in your accounts connected to such service.

Through our mobile application, data about the installed and downloaded applications in your device, which is used for security analysis and detection and prevention of malicious acts.

3.3 **Cookies.** We and our third-party partners may collect Personal Data using cookies, which are small files of letters and numbers that we store on your browser or the hard drive of your computer. We may also use pixel tags and web beacons on our Services. These are tiny graphic images placed on web pages or in our emails that allow us to determine whether you have performed a specific action. We use cookies, beacons, invisible tags, and similar technologies (collectively "**Cookies**") to collect information about your browsing activities and to distinguish you from other users of our Services. This aids your experience when you use our Services and allows us to improve the functionality of our Services. Cookies can be used for performance management, collecting information on how our Services are being used for analytics purposes. They can also be used for functionality management, enabling us to make your visit more efficient by, for example, remembering language preferences, passwords, and log-in details. For more information on the types of Cookies we and third parties may use in connection with our Services, please see our Check Point Cookies Notice (/privacy/cookies/).

How to Block Cookies. You can block Cookies by setting your internet browser to block some or all Cookies. However, if you use your browser settings to block all Cookies (including essential Cookies) you may not be able to access all or parts

of our Services. By using our Services, you consent to our use of Cookies and our processing of Personal Data collected through such Cookies, in accordance with this Privacy Policy. You can withdraw your consent at any time by deleting placed Cookies and disabling Cookies in your browser, or as explained below. You can change your browser settings to block or notify you when you receive a Cookie, delete Cookies, or browse our Services using your browser's anonymous usage setting. Please refer to your browser instructions or help screen to learn more about how to adjust or modify your browser settings. If you do not agree to our use of Cookies, you should change your browser settings accordingly. You should understand that some features of our Services may not function properly if you do not accept Cookies. Where required by applicable law, you will be asked to consent to certain Cookies before we use or install them on your computer or other device.

3.4 **Anonymized data.** In addition to the categories of Personal Data described above, Check Point may also process further anonymized information or de-identified and aggregated with other data that is not processed by reference to a specific individual.

3.5 **Careers.** In order for us to consider your application for a position with us it will be necessary for us to process certain personal data relating to you. We process personal data in accordance with applicable legislation, while considering and balancing the relevant interests of our applicants, ourselves, and other stakeholders.

4. HOW WE USE YOUR INFORMATION

4.1 We may process your Personal Data for the following purposes ("Permitted Purposes"):

for ongoing review and improvement of the information provided on Check Point Websites to ensure they are user friendly and to prevent any potential disruptions or cyberattacks;

to allow you to use and access the functionality provided by the Check Point Products and the Check Point Services;

to assess your application for Check Point Products and Check Point Services, where applicable;

to set up customers to use Check Point Products and Check Point Services;

to set up users to use the User Center;

to conduct analysis required to detect malicious data and understand how this may affect your IT system;

for statistical monitoring and analysis of current attacks on devices and systems and for the on-going adaptation of the solutions provided to secure devices and systems against current attacks;

to understand feedback on Check Point Products and Check Point Services and to help provide more information on the use of those products and services quickly and easily;

to communicate with you in order to provide you with: (i) our Services; (ii) information about us and our Services; or (iii) offers and marketing information;

to send you e-mail updates on the latest cyber security trends, news, upcoming events and other marketing or promotional materials;

for in-depth threat analysis;

to understand your needs and interests;

for the management and administration of our business;

for improvement of our products and services.

to comply with and to assess compliance with applicable laws, rules and regulations, and internal policies and procedures;

for the administration and maintenance of databases storing Personal Data to market Check Point's products and services; or

for back-up and data loss prevention.

4.2 When we process Personal Data we verify the existence of a lawful ground for such processing activity, including:

performing our contractual obligations;

a lawful consent has been obtained;

compliance with legal or regulatory obligation;

exercising or defending our rights;

legitimate business interests, such as:

- effectively and efficiently manage and administer the operation of our business;
- maintaining compliance with internal policies and procedures;
- monitoring the use of our copyrighted materials;
- enabling quick and easy access to information on our Services;
- offering optimal, up-to-date security solutions;
- sending you e-mail updates on our Services, the latest cyber security trends, news, upcoming events and other marketing or promotional materials; and
- obtaining further knowledge of current threats to network security in order to update our security solutions and provide these to the market.

4.3 As part of our Services and/or Products, we may utilize artificial intelligence (AI) technologies to enhance our capabilities and provide you with a better experience.

4.4 We will take steps to ensure that your Personal Data is accessed only by such individuals that have a need to do so for the purposes described in this Privacy Policy.

4.5 We do not retain, use, sell or disclose Personal Data for any purpose other than for the specific purpose of performing our Services or as otherwise strictly permitted under this Privacy Policy.

5. DISCLOSURE OF INFORMATION TO THIRD PARTIES

We may share or otherwise disclose the Personal Data we collect from you as described below or otherwise disclosed to you at the time of the collection.

Vendors and Service Providers. We may share any information we receive with vendors and service providers retained in connection with the provision and

marketing of our Services or other relevant services.

Partners and Affiliates. We may share any information with our distributors, partners, corporate affiliates, parents, or subsidiaries for any purpose described in this Privacy Policy.

As Required by Law and Similar Disclosures. We may access, preserve, and disclose your Personal Data if we believe doing so is required or appropriate to: (i) comply with law enforcement requests and legal process, such as a court order or subpoena; (ii) respond to your requests; or (iii) protect your, our, or others' rights, property, or safety.

Merger, Sale, or Other Asset Transfers. We may disclose and transfer your Personal Data to service providers, advisors, potential transactional partners, or other third parties in connection with the consideration, negotiation, or completion of a corporate transaction in which we are acquired by or merged with another company, or we sell, liquidate, or transfer all or a portion of our business or assets.

Consent. We may also disclose Personal Data from or about you or your devices with your permission.

6. INTERNATIONAL TRANSFERS OF PERSONAL DATA

6.1 Check Point is a global business. Our customers and our operations are spread around the world. As a result, we collect and transfer Personal Data on a global basis. That means that we may transfer your Personal Data to locations outside of your country.

6.2 Europe. Where we transfer your Personal Data to another country outside the European Economic Area ("EEA") or the United Kingdom ("UK"), we will ensure that it is protected and transferred in a manner consistent with legal requirements. In relation to data being transferred outside of Europe or the UK, for example, this may be done in one of the following ways:

the country that we send the data to, might be approved by the European Commission as offering an adequate level of protection for Personal Data (for example, Israel is an approved country);

the recipient might have signed a contract based on applicable "model contractual clauses" approved by the European Commission, obliging them to

protect your Personal Data; or

in other circumstances the law may permit us to otherwise transfer your Personal Data outside the EEA or UK.

You can obtain more details of the protection given to your Personal Data when it is transferred outside the EEA or the UK (including a copy of the standard data protection clauses which we have entered into with recipients of your Personal Data) by contacting us as described in paragraph 13 below.

6.3 China. For residents in the mainland of the People's Republic of China ("Mainland China"), we may transfer, access or store your Personal Data outside of the Mainland China where we are satisfied that adequate levels of protection are in place to protect the integrity and security of your Personal Data or adequate security measures are adopted and in compliance with the applicable laws, such as contractual arrangements. Where required by applicable laws, we will put in place appropriate measures to ensure that all processing of your Personal Data outside of the Mainland China is safeguarded by the equivalent level of data protection in the Mainland China.

7. YOUR RIGHTS

7.1 **Marketing Communications**. You can unsubscribe from our promotional emails via the link provided in the emails. Even if you opt out of receiving promotional messages from us, you will continue to receive administrative messages from us.

7.2 **Do Not Track**. There is no accepted standard on how to respond to Do Not Track signals, and we do not respond to such signals.

If you choose not to provide us with the Personal Data we collect, some features of our Services may not work as intended.

7.3 **California Privacy Rights**. If you are a California resident, you can review our California Resident Privacy Notice (/privacy/ccpa-notice/) for information about your privacy rights and choices under California law.

7.4 **Your European Privacy Rights**. If you are located in the EEA or the UK, you have additional rights described below.

You may request access the Personal Data we maintain about you, update and correct inaccuracies in your Personal Data, restrict or object to the processing of your Personal Data, have your Personal Data anonymized or deleted, as appropriate, or exercise your right to data portability to easily transfer your Personal Data to another company. In addition, you also have the right to lodge a complaint with a supervisory authority, including in your country of residence, place of work or

You may withdraw any consent you previously provided to us regarding the processing of your Personal Data at any time and free of charge. We will apply your preferences going forward and this will not affect the lawfulness of the processing before you withdrew your consent.

You may exercise these rights by contacting us using the contact details at the end of this Privacy Policy. Before fulfilling your request, we may ask you to provide reasonable information to verify your identity. Please note that there are exceptions and limitations to each of these rights, and that while any changes you make will be reflected in active user databases instantly or within a reasonable period of time, we may retain Personal Data for backups, archiving, prevention of fraud and abuse, analytics, satisfaction of legal obligations, or where we otherwise reasonably believe that we have a legitimate reason to do so.

7.5 **Other Privacy Rights.** At Check Point, we strive to uphold the highest standards of data protection and privacy compliance across various regions. If you believe you have other privacy rights relevant to a certain geographical jurisdiction, which is not covered in our policy, we encourage you to get in touch with our team at privacy_inquiries@checkpoint.com (mailto:privacy_inquiries@checkpoint.com)

8. HOW WE SAFEGUARD YOUR INFORMATION

8.1. We have extensive controls in place to maintain the security of our information and information systems. Files are protected with safeguards according to the sensitivity of the relevant information. Appropriate controls (such as restricted access) are placed on our computer systems. Physical access to areas where Personal Data is gathered, processed or stored is limited to authorized employees. In addition, our Incident Response Team plays a critical role in our commitment to safeguard your information, as they are responsible for promptly and effectively responding to data security threats. If you have a suspicion of any data breach, security incident or if you wish to report a vulnerability, please contact our team at privacy_inquiries@checkpoint.com (mailto:privacy_inquiries@checkpoint.com).

8.2 As a condition of employment, Check Point employees are required to follow all applicable laws and regulations, including in relation to data protection law. Access to sensitive Personal Data is limited to those employees who need it to perform their roles. Unauthorized use or disclosure of confidential information by a Check Point employee is prohibited and may result in disciplinary measures.

8.3 Check Point requires its worldwide employees and contractors that have access to its internal systems to complete annual trainings on data protection and security. Such trainings are aimed to make sure that Check Point's personnel understand and follow Check Point's privacy policies and guidelines when handling Personal Data.

8.4 When you contact a Check Point representative, you may be asked for some Personal Data. This type of safeguard is designed to ensure that only you, or someone authorized by you, has access to your file.

8.5. For more information on the security measures taken by Check Point in order to protect your Personal Data, please see our Security Measures Policy (/privacy/security/).

9. THIRD PARTIES

Our Services may contain links to other websites, products, or services that we do not own or operate ("Third-Party Services"). We are not responsible for the privacy practices, policies, or other content of these Third-Party Services. Please be aware that this Privacy Policy does not apply to your activities on these Third-Party Services or any information you disclose to these Third-Party Services. If you have any questions about how these other sites use your Personal Data, you should contact them directly. We encourage you to read their privacy policies before providing any information to them.

10. HOW LONG WE KEEP YOUR PERSONAL DATA

Check Point retains Personal Data only for the duration necessary to fulfill the Permitted Purposes for which it was collected. Subsequently, such data will either be destroyed, deleted, anonymized, or removed from our systems. We take measures to delete your Personal Data or keep it in a form that does not permit identifying you when this information is no longer necessary for the purposes for which we process it unless we are required by law to keep this information for a longer period. When we process Personal Data for our own purposes, we determine the retention period taking into account various criteria, such as the type of services provided to you, the nature and length of our relationship with you, possible re-enrollment with our Services, the impact on our Services we provide to you if we delete some information from or about you, and mandatory retention periods provided by law and the statute of limitations.

11. CHILDREN'S PRIVACY

We do not knowingly collect, maintain, or use Personal Data from children under 16 years of age ("**Minors**"), and no parts of our Services are directed at children. If you learn that a Minor has provided us with Personal Data in violation of this Privacy Policy, please alert us at privacy_inquiries@checkpoint.com (mailto:privacy_inquiries@checkpoint.com?subject=Children%27s%20Privacy).

12. QUESTIONS, CONCERNS AND UPDATES

If you have any questions or concerns about Check Point's handling of your Personal Data, or about this Policy, please contact our Privacy Officer using the following contact information:

Address:	Check Point Software Technologies Ltd., 5 Shlomo Kaplan Street, Tel Aviv 67897, Israel Attention: Legal Department
Address in the EU:	Check Point Software Technologies GmbH, Oskar-Messter-Str. 13, 85737, Ismaning Germany
Email Address:	privacy_inquiries@checkpoint.com (mailto:privacy_inquiries@checkpoint.com)

We are typically able to resolve privacy questions or concerns promptly and effectively. If you are not satisfied with the response you receive from our Privacy Officer, you may escalate concerns to the applicable privacy regulator in your jurisdiction. Upon request, Check Point's Data Protection Officer will provide you with the contact information for that regulator.

We will post any adjustments to the Privacy Policy on this page, and the revised version will be effective when it is posted.

You can view our Data Processing Agreement (DPA) online – Customers (/customersdpa/); Distributors and Resellers (/downloads/partners/partners-dpa.pdf). If you need a signed copy of the DPA, you can download it, send a signed copy to privacy_inquiries@checkpoint.com (mailto:privacy_inquiries@checkpoint.com) and we will provide you a countersigned copy.