

DATA PRIVACY AGREEMENT

Albany-Schoharie-Schenectady-Saratoga BOCES

and

CareerSafe, LLC

This Data Privacy Agreement ("DPA") is by and between the Albany-Schoharie-Schenectady-Saratoga BOCES ("EA"), an Educational Agency, and CareerSafe, LLC ("Contractor"), collectively, the "Parties".

ARTICLE I: DEFINITIONS

As used in this DPA, the following terms shall have the following meanings:

1. **Breach:** The unauthorized acquisition, access, use, or disclosure of Personally Identifiable Information in a manner not permitted by State and federal laws, rules and regulations, or in a manner which compromises its security or privacy, or by or to a person not authorized to acquire, access, use, or receive it, or a Breach of Contractor's security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personally Identifiable Information.
2. **Commercial or Marketing Purpose:** means the sale, use or disclosure of Personally Identifiable Information for purposes of receiving remuneration, whether directly or indirectly; the sale, use or disclosure of Personally Identifiable Information for advertising purposes; or the sale, use or disclosure of Personally Identifiable Information to develop, improve or market products or services to students.
3. **Disclose:** To permit access to, or the release, transfer, or other communication of personally identifiable information by any means, including oral, written or electronic, whether intended or unintended.
4. **Education Record:** An education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.
5. **Educational Agency:** As defined in Education Law 2-d, a school district, board of cooperative educational services, school, charter school, or the New York State Education Department.
6. **Eligible Student:** A student who is eighteen years of age or older.
7. **Encrypt or Encryption:** As defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule at 45 CFR 164.304, means the use of an algorithmic process to transform Personally Identifiable Information into an unusable, unreadable, or indecipherable form in which there is a low probability of assigning meaning without use of a confidential process or key.
8. **NIST Cybersecurity Framework:** The U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.
9. **Parent:** A parent, legal guardian or person in parental relation to the Student.

- 10. Personally Identifiable Information (PII):** Means personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g , and Teacher or Principal APPR Data, as defined below.
- 11. Release:** Shall have the same meaning as Disclose.
- 12. School:** Any public elementary or secondary school including a charter school, universal pre-kindergarten program authorized pursuant to Education Law § 3602-e, an approved provider of preschool special education, any other publicly funded pre-kindergarten program, a school serving children in a special act school district as defined in Education Law § 4001, an approved private school for the education of students with disabilities, a State-supported school subject to the provisions of Article 85 of the Education Law, or a State-operated school subject to the provisions of Articles 87 or 88 of the Education Law.
- 13. Student:** Any person attending or seeking to enroll in an Educational Agency.
- 14. Student Data:** Personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g.
- 15. Subcontractor:** Contractor’s non-employee agents, consultants and/or subcontractors engaged in the provision of services pursuant to the Service Agreement.
- 16. Teacher or Principal APPR Data:** Personally Identifiable Information from the records of an Educational Agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§ 3012-c and 3012-d.

ARTICLE II: PRIVACY AND SECURITY OF PII

1. Compliance with Law.

In order for Contractor to provide certain services ("Services") to the EA pursuant to a contract dated 10/4/2021 ("Service Agreement"); Contractor may receive PII regulated by several New York and federal laws and regulations, among them, the Family Educational Rights and Privacy Act ("FERPA") at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); New York Education Law Section 2-d; and the Commissioner of Education’s Regulations at 8 NYCRR Part 121. The Parties enter this DPA to address the requirements of New York law. Contractor agrees to maintain the confidentiality and security of PII in accordance with applicable New York, federal and local laws, rules and regulations.

2. Authorized Use.

Contractor has no property or licensing rights or claims of ownership to PII, and Contractor must not use PII for any purpose other than to provide the Services set forth in the Service Agreement.

Neither the Services provided nor the manner in which such Services are provided shall violate New York law.

3. Data Security and Privacy Plan.

Contractor shall adopt and maintain administrative, technical and physical safeguards, measures and controls to manage privacy and security risks and protect PII in a manner that complies with New York State, federal and local laws and regulations and the EA's policies. Education Law Section 2-d requires that Contractor provide the EA with a Data Privacy and Security Plan that outlines such safeguards, measures and controls including how the Contractor will implement all applicable state, federal and local data security and privacy requirements. Contractor's Data Security and Privacy Plan is attached to this DPA as Exhibit C.

4. EA's Data Security and Privacy Policy

State law and regulation requires the EA to adopt a data security and privacy policy that complies with Part 121 of the Regulations of the Commissioner of Education and aligns with the NIST Cyber Security Framework. Contractor shall comply with the EA's data security and privacy policy and other applicable policies.

5. Right of Review and Audit.

Upon request by the EA, Contractor shall provide the EA with copies of its policies and related procedures that pertain to the protection of PII. It may be made available in a form that does not violate Contractor's own information security policies, confidentiality obligations, and applicable laws. In addition, Contractor may be required to undergo an audit of its privacy and security safeguards, measures and controls as it pertains to alignment with the requirements of New York State laws and regulations, the EA's policies applicable to Contractor, and alignment with the NIST Cybersecurity Framework performed by an independent third party at Contractor's expense, and provide the audit report to the EA. Contractor may provide the EA with a recent industry standard independent audit report on Contractor's privacy and security practices as an alternative to undergoing an audit.

6. Contractor's Employees and Subcontractors.

- (a) Contractor shall only disclose PII to Contractor's employees and subcontractors who need to know the PII in order to provide the Services and the disclosure of PII shall be limited to the extent necessary to provide such Services. Contractor shall ensure that all such employees and subcontractors comply with the terms of this DPA.
- (b) Contractor must ensure that each subcontractor performing functions pursuant to the Service Agreement where the subcontractor will receive or have access to PII is contractually bound by a written agreement that includes confidentiality and data security obligations equivalent to, consistent with, and no less protective than, those found in this DPA.

- (c) Contractor shall examine the data security and privacy measures of its subcontractors prior to utilizing the subcontractor. If at any point a subcontractor fails to materially comply with the requirements of this DPA, Contractor shall: notify the EA and remove such subcontractor's access to PII; and, as applicable, retrieve all PII received or stored by such subcontractor and/or ensure that PII has been securely deleted and destroyed in accordance with this DPA. In the event there is an incident in which the subcontractor compromises PII, Contractor shall follow the Data Breach reporting requirements set forth herein.
- (d) Contractor shall take full responsibility for the acts and omissions of its employees and subcontractors.
- (e) Contractor must not disclose PII to any other party unless:
 - (i) The Contractor has received written permission from a parent or eligible student to whom the data pertains to beforehand; or
 - (ii) Such disclosure is required by statute, court order or subpoena, and the Contractor makes a reasonable effort to notify the EA of the court order or subpoena in advance of compliance but in any case, provides notice to the EA no later than the time the PII is disclosed, unless such disclosure to the EA is expressly prohibited by the statute, court order or subpoena.

7. Training.

Contractor shall ensure that all its employees and Subcontractors who have access to PII have received or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access.

8. Termination

The obligations of this DPA shall continue and shall not terminate for as long as the Contractor or its sub-contractors retain PII or retain access to PII.

9. Data Return and Destruction of Data.

- (a) Protecting PII from unauthorized access and disclosure is of the utmost importance to the EA, and Contractor agrees that it is prohibited from retaining PII or continued access to PII or any copy, summary or extract of PII, on any storage medium (including, without limitation, in secure data centers and/or cloud-based facilities) whatsoever beyond the period of providing Services to the EA, unless such retention is either expressly authorized for a prescribed period by the Service Agreement or other written agreement between the Parties, or expressly requested by the EA for purposes of facilitating the transfer of PII to the EA or expressly required by law.
- (b) Contractor shall provide the EA with a written certification of the secure deletion and/or destruction of PII held by the Contractor or Subcontractors.

- (c) To the extent that Contractor and/or its subcontractors continue to be in possession of any de-identified data (i.e., data that has had all direct and indirect identifiers removed), they agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party.

10. Commercial or Marketing Use Prohibition.

Contractor agrees that it will not sell PII or use or disclose PII for a Commercial or Marketing Purpose.

11. Encryption.

Contractor shall use industry standard security measures including encryption protocols that comply with New York law and regulations to preserve and protect PII. Contractor must encrypt PII at rest and in transit in accordance with applicable New York laws and regulations.

12. Breach.

- (a) Contractor shall promptly notify the EA of any Breach of PII without unreasonable delay no later than seven (7) business days after discovery of the Breach. Notifications required pursuant to this section must be in writing, given by personal delivery, e-mail transmission (if contact information is provided for the specific mode of delivery), or by registered or certified, and must to the extent available, include a description of the Breach which includes the date of the incident and the date of discovery; the types of PII affected and the number of records affected; a description of Contractor’s investigation; and the contact information for representatives who can assist the EA. Notifications required by this section must be sent to the EA’s District Superintendent or other head administrator with a copy to the Data Protection Office. Violations of the requirement to notify the EA shall be subject to a civil penalty pursuant to Education Law Section 2-d. The Breach of certain PII protected by Education Law Section 2-d may subject the Contractor to additional penalties.
- (b) Notifications required under this paragraph must be provided to the EA at the following address:

Name: Michele Jones

Title: Data Protection Officer

Address: 900 Watervliet-Shaker Road

City, State, Zip: Albany, NY 12205

Email: dpo@neric.org

13. Cooperation with Investigations.

Contractor agrees that it will cooperate with the EA and law enforcement, where necessary, in any investigations into a Breach. Any costs incidental to the required cooperation or participation of the Contractor or its' Authorized Users, as related to such investigations, will be the sole responsibility of the Contractor if such Breach is attributable to Contractor or its Subcontractors.

14. Notification to Individuals.

Where a Breach of PII occurs that is attributable to Contractor, Contractor shall pay for or promptly reimburse the EA for the cost of the EA's notification to Parents, Eligible Students, teachers, and/or principals, in accordance with Education Law Section 2-d and 8 NYCRR Part 121. The cost is limited up to the coverage limited by the Contractor's Cyber Liability Insurance.

15. Termination.

The confidentiality and data security obligations of the Contractor under this DPA shall survive any termination of this DPA but shall terminate upon Contractor's certifying that it has destroyed all PII.

ARTICLE III: PARENT AND ELIGIBLE STUDENT PROVISIONS

1. Parent and Eligible Student Access.

Education Law Section 2-d and FERPA provide Parents and Eligible Students the right to inspect and review their child's or the Eligible Student's Student Data stored or maintained by the EA. To the extent Student Data is held by Contractor pursuant to the Service Agreement, Contractor shall respond within thirty (30) calendar days to the EA's requests for access to Student Data so the EA can facilitate such review by a Parent or Eligible Student, and facilitate corrections, as necessary. If a Parent or Eligible Student contacts Contractor directly to review any of the Student Data held by Contractor pursuant to the Service Agreement, Contractor shall promptly notify the EA and refer the Parent or Eligible Student to the EA.

2. Bill of Rights for Data Privacy and Security.

As required by Education Law Section 2-d, the Parents Bill of Rights for Data Privacy and Security and the supplemental information for the Service Agreement are included as Exhibit A and Exhibit B, respectively, and incorporated into this DPA. Contractor shall complete and sign Exhibit B and append it to this DPA. Pursuant to Education Law Section 2-d, the EA is required to post the completed Exhibit B on its website.

ARTICLE IV: MISCELLANEOUS

1. Priority of Agreements and Precedence.

In the event of a conflict between and among the terms and conditions of this DPA, including all Exhibits attached hereto and incorporated herein and the Service Agreement, the terms and conditions of this DPA shall govern and prevail, shall survive the termination of the Service Agreement in the manner set forth herein, and shall supersede all prior communications, representations, or agreements, oral or written, by the Parties relating thereto.

2. Execution.

This DPA may be executed in one or more counterparts, all of which shall be considered one and the same document, as if all parties had executed a single original document, and may be executed utilizing an electronic signature and/ or electronic transmittal, and each signature thereto shall be and constitute an original signature, as if all parties had executed a single original document.

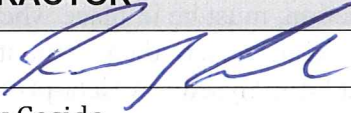
EDUCATIONAL AGENCY	CONTRACTOR
BY: <i>[Signature]</i>	BY: 
<i>[Printed Name]</i>	Rodney Casida
[Title]	CFO
Date:	Date: 10/4/2021

EXHIBIT A - Education Law §2-d Bill of Rights for Data Privacy and Security
PARENT BILL OF RIGHTS

Albany-Schoharie-Schenectady-Saratoga BOCES (Capital Region BOCES), in recognition of the risk of identity theft and unwarranted invasion of privacy, affirms its commitment to safeguarding student personally identifiable information (PII) in educational records from unauthorized access or disclosure in accordance with State and Federal law. BOCES establishes the following parental bill of rights:

- Student PII will be collected and disclosed only as necessary to achieve educational purposes in accordance with State and Federal Law.
- A student's personally identifiable information cannot be sold or released for any marketing or commercial purposes by BOCES or any a third party contractor. BOCES will not sell student personally identifiable information and will not release it for marketing or commercial purposes, other than directory information released by BOCES in accordance with BOCES policy;
- Parents have the right to inspect and review the complete contents of their child's education record (for more information about how to exercise this right, see 5500-R);
- State and federal laws, such as NYS Education Law §2-d and the Family Educational Rights and Privacy Act, protect the confidentiality of students' personally identifiable information. 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;
- A complete list of all student data elements collected by the State Education Department is available for public review at <http://nysed.gov/data-privacy-security> or by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.
- Parents have the right to have complaints about possible breaches and unauthorized disclosures of student data addressed. Complaints should be directed to the Data Protection Officer, (518) 464-5139, DPO@neric.org, Capital Region BOCES, 900 Watervliet-Shaker Rd., Albany NY 12205. Complaints can also be directed to the New York State Education Department online at <http://nysed.gov/data-privacy-security> by mail to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234 or by email to privacy@mail.nysed.gov or by telephone at 518-474-0937.
- Parents have the right to be notified in accordance to applicable laws and regulations if a breach or unauthorized release of their student's PII occurs.
- Parents can expect that educational agency workers who handle PII will receive annual training on applicable federal and state laws, regulations, educational agency's policies and safeguards which will be in alignment with industry standards and best practices to protect PII.
- In the event that BOCES engages a third party provider to deliver student educational services, the contractor or subcontractors will be obligated to adhere to State and Federal Laws to safeguard student PII. Parents can request information about third party contractors by contacting the Data Protection Officer, (518)-464-5139, DPO@neric.org, 900 Watervliet-Shaker Rd., Albany NY 12205, or can access the information on BOCES' website <https://www.capitalregionboces.org/>.

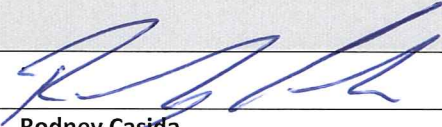
CONTRACTOR	
[Signature]	
[Printed Name]	Rodney Casida
[Title]	CFO
Date:	10/9/2021

EXHIBIT B

BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY - SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE INFORMATION

Pursuant to Education Law § 2-d and Section 121.3 of the Commissioner’s Regulations, the Educational Agency (EA) is required to post information to its website about its contracts with third-party contractors that will receive Personally Identifiable Information (PII).

Name of Contractor	CareerSafe, LLC
Description of the purpose(s) for which Contractor will receive/access PII	We develop and sell online, web based OSHA 10 hour courses as well as other technical and life skill courses. The purpose for the access to PII is for students to obtain their OSHA 10 hour certification as well as complete our other courses
Type of PII that Contractor will receive/access	Check all that apply: <input checked="" type="checkbox"/> Student PII <input type="checkbox"/> APPR Data
Contract Term	Contract Start Date <u>10/4/2021</u> Contract End Date <u>10/3/2024</u>
Subcontractor Written Agreement Requirement	Contractor will not utilize subcontractors without a written contract that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Contract. (check applicable option) <input checked="" type="checkbox"/> Contractor will not utilize subcontractors. <input type="checkbox"/> Contractor will utilize subcontractors.
Challenges to Data Accuracy	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. If a correction to data is deemed necessary, the EA will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA’s written request.
Secure Storage and Data Security	Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply) <input checked="" type="checkbox"/> Using a cloud or infrastructure owned and hosted by a third party.

	<input type="checkbox"/> Using Contractor owned and hosted solution <input type="checkbox"/> Other: Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data: FIPS 140-2 compliant / certified process used to encrypt the student data while at rest on the application database. Student data is stored in/on an application database, located in the Amazon Web Services hosting facilities. The back-up data is presently stored on site in a secured storage unit.
Encryption	Data will be encrypted while in motion and at rest.

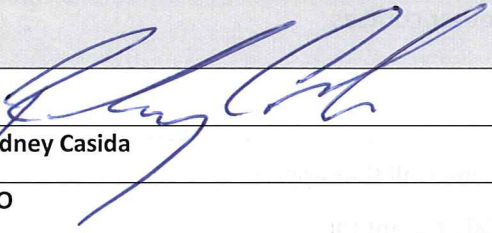
CONTRACTOR	
[Signature]	
[Printed Name]	Rodney Casida
[Title]	CFO
Date:	10/4/2021

EXHIBIT C - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

The Educational Agency (EA) is required to ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan, pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations. For every contract, the Contractor must complete the following or provide a plan that materially addresses its requirements, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York state. **While this plan is not required to be posted to the EA's website, contractors should nevertheless ensure that they do not include information that could compromise the security of their data and data systems.**

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	<p>CareerSafe Online follows NIST standards for data security and privacy. In addition to NIST, CareerSafe Online maintains certification through ikeepsafe.com. We are currently tested and approved for FERPA, COPPA and CSPC within that program. This certification includes 3rd party technical assessment of our systems as well as detailed assessment of our privacy controls. We intend to maintain this high level of compliance to protect all of our clients.</p>
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	<p>FIPS 140-2 compliant / certified process used to encrypt the student data while at rest on the application database.</p> <p>We use above industry-standard security practices to protect data. All CareerSafe system administrators are fully vetted via criminal background checks at hiring and full background investigations from the Department of Education. Our system administrators use built-in operating system controls to prevent information leakage between users or processes acting on behalf of users, including both concurrent users as well as prior and future users. Additionally, our hosting environment and infrastructure is FedRamp certified and is held to the highest security standards including</p>

		continuous monitoring, control testing and assessment, monthly vulnerability scanning, tec. All data is fully encrypted to an AES 256 bit standard at rest and while in transit. All backups are encrypted and stored in a secured SCIF that is only accessible by CareerSafe security personnel.
3	Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.	All of our employees are trained in data privacy and the handling of PII. Additionally, our security team attends annual training on Risk Management, PII handling, industry standard certifications (CISSP, CISM, PMP) that focus on security. Our operations team focuses on the security of the hosting environments and hold many industry recognized professional certifications.
4	Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.	All CareerSafe system administrators are fully vetted via criminal background checks at hiring and full background investigations from the Department of Education. We do not use subcontractors.
5	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the EA.	CareerSafe Online has a clearly defined Privacy Policy that details how we handle data and how we will respond to any PII spillage event. This can be found on the CareerSafeonline.com page. Additionally, we have an internal spillage procedure that all employees are trained to follow so that we have a consistent response.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Each EA is contracted separately so there is no "one size fits all" rule. Generally, the transition rules are detailed in the contract. In a nutshell, CareerSafe Online will securely provide any data requested at the end of the contract and irrevocably destroy any data on the CareerSafe Online system. Details would be provided by the EA.

		As an authorized OSHA Vendor, student completion records must be maintained for five years. After which, CareerSafe will destroy and delete all the data in its entirety in the manner that prevents its physical reconstruction.
7	Describe your secure destruction practices and how certification will be provided to the EA.	Student completion records will be maintained for five years, after which, CareerSafe will destroy and delete all the data in its entirety in the manner that prevents its physical reconstruction.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	Based on a basic review of the EA's policies for data security and privacy, CareerSafe Online meets or exceeds requirements. Policies and practices align.
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below.	PLEASE USE TEMPLATE BELOW.

EXHIBIT C.1 – NIST CSF TABLE

The table below will aid the review of a Contractor's Data Privacy and Security Plan. Contractors should complete the Contractor Response sections in the table below to describe how their policies and practices align with each category in the Data Privacy and Security Plan template. To complete these 23 sections, a Contractor may: (i) Demonstrate alignment using the National Cybersecurity Review (NCSR) Maturity Scale of 1-7 ; (ii) Use a narrative to explain alignment (may reference its applicable policies); and/or (iii) Explain why a certain category may not apply to the transaction contemplated. Further informational references for each category can be found on the NIST website at <https://www.nist.gov/cyberframework/new-framework>. Please use additional pages if needed.

Function	Category	Contractor Response
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative	CM-2, CM-6, CM-8, CM-8(1): The CareerSafe System Owner works with the configuration management team (Quality Assurance) ensure that accurate system documentation and configuration logs are maintained to reflect current and prior configuration baselines. A current baseline of the support server operating

Function	Category	Contractor Response
	importance to organizational objectives and the organization's risk strategy.	<p>systems and application software is maintained and is referenced as part of our patch management process.</p> <p>The inventory of information system components is maintained and includes manufacturer, type, serial number, version number, and location (i.e., physical location and logical position within the information system architecture). Furthermore, changes to the existing configuration will be updated using the change management process as an integral part of information system component installations.</p> <p>AC-4: All K2share applications enforce an approved system design to control the flow of information within the system. Data flows must ensure a tiered structure that provides interconnections of the component services. This ensures that each system function operates within its own standard services and protocols and that one communications protocol cannot be used to access another service.</p> <p>Data flows between system components are based on information flow control designs approved by the K2share IT and Security Teams. All system interconnections are managed with access control lists (ACLs), Internet Protocol (IP) address lists, virtual private networks (VPNs), network segmentation, and similar functions. Each system's technical description contains flow diagrams and expresses the information flow and its enforcement mechanisms.</p>
	<p>Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.</p>	<p>CareerSafe Online has a dedicated Security Officer that manages the security practices within the program. The Security Officer reports directly to executive management and is designated to make security related decisions for the program. The Security Officer works closely with the IT Director, Development Manager, Executive Team, and Program Management to ensure that all regulations, privacy laws, policies, and procedures are followed and that the Risk Management program is understood and followed. The Security Officer role is assigned to a security professional in the company.</p>
	<p>Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.</p>	<p>CareerSafe Online has a dedicated Security Officer that manages the security practices within the program. The Security Officer reports directly to executive management and is designated to make security related decisions for the program. The Security Officer works closely with the IT Director, Development Manager, Executive Team, and Program Management to ensure that all regulations, privacy laws, policies, and procedures are followed and that the Risk Management program is understood and followed. The Security Officer role is assigned to a security professional in the company.</p>
	<p>Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.</p>	<p>RA-3: K2Share has implemented a continuous monitoring and risk assessment strategy. The Risk Register in Jira is a tool that allows the organization to continuously tracks risks to the organization. K2Share conducts formal risk assessments in compliance with the NIST RMF process. The process includes annual and ad-hoc reviews and updates.</p> <p>RA-5: K2Share performs monthly scans for vulnerabilities in the information system and hosted applications using credentialed vulnerability scan. These scans are performed for continuous monitoring, configuration management, and when new vulnerabilities potentially affecting the system/applications are identified and reported. The tester employs the Tenable Nessus tool to perform the vulnerability management process. The System Administrator is responsible for maintaining this control</p>

Function	Category	Contractor Response
		<p>and it will be reviewed annually, or when there is a significant change to the system. There are reviews of all monthly scan and assessment reports; findings are addressed per the K2Share patch and vulnerability management guidance. The systems Configuration Management Plan contains the Vulnerability and Patch Management guidance.</p> <p>CA-2, CA-5, CA-7: K2Share has implemented a continuous monitoring and assessment strategy. The Risk Register in Jira is a tool that allows the organization to continuously tracks risks to the organization. If the Security or Operations teams detect a flaw or deficiency, they can either create a Risk Register item or an ITHelp ticket to track the remediation of this vulnerability.</p>
	<p>Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.</p>	<p>The CareerSafe Online Risk Management Process consists of:</p> <ul style="list-style-type: none"> • Defining and framing the context of decisions and related goals and objectives • Identifying the risks associated with the goals and objectives Analyzing and assessing the identified risks • Developing alternative actions for managing the risks and creating opportunities and analyzing the costs and benefits of those alternatives • Making a decision among alternatives and implementing that decision • Monitoring the implemented decision and comparing observed and expected effects to help influence subsequent risk management alternatives and decisions. <p>CareerSafe Online has also developed an appropriate mitigation plan that involves consideration of different mitigation strategies. Our security staff ensures that the mitigation progress is tracked and regularly reported to upper management; management ensures that planned mitigation achieves the desired result and, if not, that they are prepared to execute an alternative mitigation or invoke a contingency plan. Contingency plans are developed with the understanding that the cost of managing a risk should be less than the projected impact of the risk.</p> <p>CareerSafe Online has implemented a Risk Management Strategy by developing a repeatable process for regularly assessing the Information Security Program's conditions in order to capture newly introduced risks. Risks and their associated data are forwarded to management in a timely manner to facilitate the decision-making process. Prompt and timely decision making is focused on ensuring that risks are controlled before negative consequences occur.</p> <p>CareerSafe Online updates the information security program annually based on the changing risks.</p>
	<p>Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are</p>	<p>CareerSafe Online understands and constantly reviews risk related activities that may affect operations, including supply chain. We have identified, as part of our Risk Management strategy, key</p>

Function	Category	Contractor Response
	<p>established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.</p>	<p>areas, and possible threats to our operations. These threats are constantly evaluated in the case of needed escalation to prevent interruption to service.</p>
<p>PROTECT (PR)</p>	<p>Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.</p>	<p>AC-2, AC-3, AC-17: <i>Identify information system account types:</i> The ISO must identify and assign privileged and non-privileged account types that are required. The selection should address both internal users and external users. The ISO should provide email approvals for privileged users including system and application administrators who will also act as the account managers. The ISO also should provide approvals for unique roles and groups needed to support business functions.</p> <p><i>Application Groups:</i> When role-based groups are needed for the application, the ISO can assign an application administrator to manage those groups. Only approved persons should have their user IDs placed in specified application roles or groups. Account assignments should be made with consideration of the actual role/function required.</p> <p><i>New Users/Accounts:</i> When a new user or account type is needed to be added to the system, the request must go via email to the ISO for approval. The ISO and/or PM will email the system and application administrators with the new user's contact information as an approval. The system and application administrators will create a unique user account for each individual.</p> <p><i>Account Changes:</i> If the user's role or function changes, the ISO and/or PM will notify the system administrator to make appropriate changes. The use of role-based access will ensure that only persons who have been properly approved will have access to privileged accounts and sensitive information.</p> <p><i>Remove or Disable Accounts:</i> Emails will be used to request removal or disabling accounts for all users who no longer have a designated role or require access to the system or application. These account changes must be made within 24 hours. Account changes should be notified via email to the ISO and/or PM to notify of completed actions. When an external user accounts are no longer needed, they should be disabled immediately.</p> <p><i>Annual User Reviews:</i> The ISO and/or PM will perform an annual review of authorized user listings to ensure that the listing is current. They will notify the system or application administrator to disable or remove any accounts that are not being used. The system logs should be reviewed on monthly basis to monitor the use and status of accounts. This can be done using access log reviews and management console views for the web application and AWS GovCloud, or via other technical means. The system and/or application administrator should review these logs on a monthly basis and an account review tracking record is recommended.</p> <p>Shared or Group accounts are prohibited at K2Share.</p> <p>AC-5: K2Share employs separation of duties for personnel to address the potential for abuse of authorized privileges. These roles and/or duties are documented to provide a description of the approved persons, the defined roles, and the assigned functions. K2Share follows a formal user account and/or role assignment process to ensure only authorized K2Share admins can access restricted functions requiring application privileges.</p> <p>K2Share Security, System Owners and HR documents and identifies individuals, duties, and their approved access. This</p>

Function	Category	Contractor Response
		record is reviewed at least on an annual basis to determine the effectiveness of the separate duty assignments.
	<p>Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.</p>	<p>AT-2, AT-3: The K2Share HR Manager provides or ensures annual Security Awareness Training to all K2Share personnel including system administrators, network administrators, database administrators, quality assurance staff and ISSO staff using vetted awareness training materials or equivalent course content. The training materials address the specific requirements of the organization and the information systems to which personnel have authorized access. Additional awareness sessions are conducted "whenever there is a significant change in the IT security environment or procedures or when an employee enters a new position involving the handling of sensitive information." The K2Share HR Manager retains copies of training schedules, training rosters, training reports, etc.</p> <p>K2Share admin personnel with significant security responsibilities (e.g., ISSOs, system administrators, etc.) receive initial specialized training from existing staff and orientation procedures dependent upon the individual's job description and duties. K2Share system administrators receive specific training according to the component(s) they support. Training has included Database tools and security, AWS management, Risk Management Framework, CISSP, CISM, Security +, F5 BigIP Load Balancer Certification, and CISCO Boot Camps. Senior managers, system owners, and IT Project Managers attend courses specific to their security responsibilities. Security management are CISSP certified and continue formal training in that area annually.</p>

Function	Category	Contractor Response
	<p>Data Security (PR.DS): Information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information.</p>	<p>All CareerSafe Online data is managed in accordance to the Risk Management plan.</p> <p>SC-4: K2Share has incorporated cloud service best practices into developing and maintaining the hosting environment. The web user interface is separated from application processing components used for the analysis and storage of customer logs. The production environment is completely segregated from other customers through the use of virtual private clouds (VPCs). Each customer is assigned their own VPC for data collection and storage. K2Share’s hosting environment is architected with a management VPC and each customer is provided their own VPC to ensure customer isolation. AWS IAM roles allow K2Share instances to only access data and components required for their function. All code development adheres to industry best practices, including expectations for input validation, parameterization, and authenticator management. K2Share developers are not allowed to hardcode authenticators into configuration scripts, or web application code in order to prevent loss of functionality if the codebase or an authenticator is modified. This prevents web-based attacks from providing access to the data tier.</p> <p>SC-8, SC-8(1): K2Share uses integrity checking on all data transmissions using protocols such as TCP/IP, checksums on data transfer, and other mechanisms if available to ensure the integrity of transmitted information.</p> <p>SC-13: K2Share requires and enforces encryption on all traffic crossing the boundary. All traffic (SSL/TLS and Remote Desktop Protocol) encryption is FIPS 140-2 compliant using FIPS 197 (AES-256) algorithms.</p> <p>SC-28: All K2Share information resides on computer-disk storage systems or on backup archives which are encrypted and accessible by only privileged system administration by means of access control restrictions enforced by operating system security rules and/or physical security controls. The storage systems are physically secured inside locked cabinets within locked server rooms with access limited to specific administrators with key card access.</p>
	<p>Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.</p>	<p>CareerSafe Online maintains and enforces security policies and procedures to protect information systems. This is the responsibility of the Information Security Officer.</p>
	<p>Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.</p>	<p>MA-2, MA-3, MA-3(1), MA-3(2): All CareerSafe Online maintenance is performed as needed when problems arise due to capacity constraints, software or hardware faults, or the need to apply a security patch or protective measure due to a security alert. The system administrator: (a.) Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or K2Share requirements; (b.) Controls all maintenance activities and performs all maintenance locally, onsite. K2Share prohibits remote maintenance and does not</p>

Function	Category	Contractor Response
		<p>remove equipment to other locations for service; (c.) Would require that a designated official explicitly approve the removal of the information system or system components from facilities for off-site maintenance or repairs in the unlikely event that became necessary; (d.) No media is removed for maintenance. If equipment is removed, all media is sanitized by using the guidance provided by NIST, including media destruction using K2Share-provided media destruction equipment; and (e.) Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions. The CareerSafe Online security personnel validate that all controls are properly functioning after maintenance. CareerSafe Online may employ automated mechanisms to schedule, conduct, and document maintenance and repairs as required, producing up-to-date, accurate, complete, and available records of all maintenance and repair actions, needed, in process, and completed. CareerSafe Online employs several automated mechanisms for ensuring timely maintenance. Patch management is a major event-driven requirement for maintenance and CareerSafe Online uses Ivanti to automate and manage patches for security and bug fixes for all servers.</p>
	<p>Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.</p>	<p>AU-2, AU-3, AU-3(1), AU-6, AU-12: K2Share systems generate audit records containing occurrence information that establishes: Event Types; Event Times; System Affected; Sources; Outcomes; and IDs. These logs are used to monitor all activity in the Managed SIEM. The audit logs contain sufficient information to establish the user's identity, what type, when and where the event occurred, source IP and success or failure of the event. K2Share AWS systems uses CloudWatch and CloudTrail to support auditing functionality. The system generates audit records for the list of audited events defined in AU-2 with the content as defined in AU-3. K2Share Servers have system policies set to enforce logging at the operating system and database management levels. K2Share allocates audit record storage capacity through the use of the AWS hosting infrastructure. This provides sufficient audit storage capacity to meet requirements. Properties for all audit-related logs are set to archive the logs when full and they must not overwrite events.</p>
DETECT (DE)	<p>Anomalies and Events (DE.AE): Anomalous activity is detected, and the potential impact of events is understood.</p>	<p>AU-6(3): All K2share system logs are forwarded to the central Syslog server, where the SEIM processes the logs for various alert conditions. If suspicious activity is identified, it automatically emails the security team and ISSO. Only the Security team is authorized to access, modify, delete audit information in the SIEM. All servers run industry recognized malware tools.</p>
	<p>Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.</p>	<p>AU-6(3): All K2share system logs are forwarded to the central Syslog server, where the SEIM processes the logs for various alert conditions. If suspicious activity is identified, it automatically emails the security team and ISSO. Only the Security team is authorized to access, modify, delete audit information in the SIEM. All servers run industry recognized malware tools. Events are constantly monitored and tested for effectiveness.</p>
	<p>Detection Processes (DE.DP): Detection processes and procedures are maintained</p>	<p>CareerSafe Online utilizes several tools including SIEM, AV, server internal logging and AWS CloudTrail to correlate detection events</p>

Function	Category	Contractor Response
	and tested to ensure awareness of anomalous events.	that are deemed a potential threat event. All of these tools are tested on a weekly basis with test scripts and known test modules. All tests are coordinated with the operations and security teams. All alerts are sent via email and logged with a ticket that is tracked to closure.
RESPOND (RS)	<p>Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.</p>	<p>The CareerSafe Online Security Officer is responsible for developing and disseminating a Contingency Plan (CP) with the guidance from the SO for the information system that: identifies essential missions and business functions and associated contingency requirements; <i>provides recovery objectives</i>, restoration priorities, and metrics; addresses contingency roles, responsibilities, assigned individuals with contact information; addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and is reviewed and approved by the CareerSafe Online Security Officer.</p> <ul style="list-style-type: none"> • The CareerSafe Online Security Officer distributes copies of the CP to all personnel with roles and responsibilities defined within the contingency plan.; • The organization coordinates contingency planning activities with incident handling activities. These coordination efforts are addressed in both the CP and the Incident Response Plan (IRP); • The CareerSafe Online Security Officer is responsible for reviewing the CP for the information system annually and. • The CareerSafe Online Security Officer is responsible for updating the CP to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing, when necessary. • CareerSafe Online communicates CP changes to all personnel with roles and responsibilities defined within the contingency plan, when necessary. • The CareerSafe Online Security Officer works through the AAR with the team to identify and document improvements to the process. <p>There are detailed sections in the Contingency Plan that identify restoration activities and timelines to be followed.</p> <ul style="list-style-type: none"> • CareerSafe Online protects the CP from unauthorized disclosure and modification.
	<p>Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).</p>	<p>As stated in entries above, CareerSafe Online maintains and updates an Incident Response plan that incorporates communications channels both internally with stakeholders and externally as required.</p>
	<p>Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.</p>	<p>The CareerSafe Online incident response team includes personnel from many areas within the organization to ensure that a thorough analysis can be made for those response efforts made by the team.</p>
	<p>Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.</p>	<p>The CareerSafe Online incident response team includes personnel from management, operations, development, and security. The personnel included in the Incident Response Team are trained to</p>

Function	Category	Contractor Response
		<p>identify items that are important to mitigate the threat and to ensure that the threat is not allowed to propagate.</p>
	<p>Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.</p>	<p>Key parts of the Risk Management and Contingency Plans are to identify and document events in an After Action Report (AAR). These AAR's are documented as an appendix and are reviewed annually to improve response activities.</p>
RECOVER (RC)	<p>Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.</p>	<p>The CareerSafe Online Security Officer is responsible for developing and disseminating a Contingency Plan (CP) with the guidance from the SO for the information system that: identifies essential missions and business functions and associated contingency requirements; <i>provides recovery objectives</i>, restoration priorities, and metrics; addresses contingency roles, responsibilities, assigned individuals with contact information; addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and is reviewed and approved by the CareerSafe Online Security Officer.</p> <ul style="list-style-type: none"> • The CareerSafe Online Security Officer distributes copies of the CP to all personnel with roles and responsibilities defined within the contingency plan.; • The organization coordinates contingency planning activities with incident handling activities. These coordination efforts are addressed in both the CP and the Incident Response Plan (IRP); • The CareerSafe Online Security Officer is responsible for reviewing the CP for the information system annually. • The CareerSafe Online Security Officer is responsible for updating the CP to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing, when necessary. • CareerSafe Online communicates CP changes to all personnel with roles and responsibilities defined within the contingency plan, when necessary. • The CareerSafe Online Security Officer works through the AAR with the team to identify and document improvements to the process. <p>CareerSafe Online protects the CP from unauthorized disclosure and modification.</p>
	<p>Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.</p>	<p>The CareerSafe Online Security Officer is responsible for developing and disseminating a Contingency Plan (CP) with the guidance from the SO for the information system that: identifies essential missions and business functions and associated contingency requirements; <i>provides recovery objectives</i>, restoration priorities, and metrics; addresses contingency roles, responsibilities, assigned individuals with contact information; addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and is reviewed and approved by the CareerSafe Online Security Officer.</p>

Function	Category	Contractor Response
		<ul style="list-style-type: none"> • The CareerSafe Online Security Officer distributes copies of the CP to all personnel with roles and responsibilities defined within the contingency plan.; • The organization coordinates contingency planning activities with incident handling activities. These coordination efforts are addressed in both the CP and the Incident Response Plan (IRP); • The CareerSafe Online Security Officer is responsible for reviewing the CP for the information system annually and. • The CareerSafe Online Security Officer is responsible for updating the CP to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing, when necessary. • CareerSafe Online communicates CP changes to all personnel with roles and responsibilities defined within the contingency plan, when necessary. • The CareerSafe Online Security Officer works through the AAR with the team to identify and document improvements to the process. <p>There are detailed sections in the Contingency Plan that identify restoration activities and timelines to be followed.</p> <p>CareerSafe Online protects the CP from unauthorized disclosure and modification.</p>
	<p>Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).</p>	<p>The CareerSafe Online Security Officer is responsible for developing and disseminating a Contingency Plan (CP) with the guidance from the SO for the information system that: identifies essential missions and business functions and associated contingency requirements; <i>provides recovery objectives</i>, restoration priorities, and metrics; addresses contingency roles, responsibilities, assigned individuals with contact information; addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and is reviewed and approved by the CareerSafe Online Security Officer.</p> <ul style="list-style-type: none"> • The CareerSafe Online Security Officer distributes copies of the CP to all personnel with roles and responsibilities defined within the contingency plan.; • The organization coordinates contingency planning activities with incident handling activities. These coordination efforts are addressed in both the CP and the Incident Response Plan (IRP); • The CareerSafe Online Security Officer is responsible for reviewing the CP for the information system annually and. • The CareerSafe Online Security Officer is responsible for updating the CP to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing, when necessary. • CareerSafe Online communicates CP changes to all personnel with roles and responsibilities defined within the contingency plan, when necessary. • The CareerSafe Online Security Officer works through the AAR with the team to identify and document improvements to the process.

Function	Category	Contractor Response
		<p>There are detailed sections in the Contingency Plan that identify restoration activities and timelines to be followed.</p> <p>CareerSafe Online protects the CP from unauthorized disclosure and modification.</p>

September 21, 2021

Addendum 1: Student Data Agreement

This addendum is being issued to append the Data Sharing Agreement (the “Agreement”) between CareerSafe, LLC (“Provider”) and Capital Region BOCES (the “District”).

Provider does not share or sell student information. The only time information is shared is through our Occupational Safety and Health Administration (OSHA) agreement as an OSHA-authorized online outreach training provider.

Provider shall maintain student records solely for the purpose of meeting regulations of OSHA as relates to documentation of credential requirements. During the five-year mandated data maintenance period, Provider agrees to maintain security of students’ personally identifiable information in accordance with this agreement. Upon the expiration of OSHA mandated five-year data maintenance period, Provider agrees to erase, destroy, and render unreadable, all data in its entirety in the manner that prevents its physical reconstruction through the use of commonly available file restoration utilities.

The Data Sharing Agreement (the “Agreement”) will be made effective upon execution of this addendum by both parties.

CareerSafe, LLC

Signature of Authorized Representative

Rodney Casida

Printed Name

CFO

Position

09/21/2021

Date

Capital Region BOCES

Signature of Authorized Representative

Printed Name

Position

Date