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	**Certiport, a business of NCS Pearson, Inc.**
Description of the purpose(s) for which Contractor will receive/access PII	**Examination account creation**
Type of PII that Contractor will receive/access	Check all that apply: ☒ Student PII ☐ APPR Data
Contract Term	Contract Start Date _____ Contract End Date _____
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) ☒ Contractor will not utilize subcontractors. ☐ Contractor will utilize subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, Contractor shall: • Securely transfer data to EA, or a successor contractor at the EA's option and written discretion, in a format agreed to by the parties. • Securely delete and destroy data.
Challenges to Data Accuracy	Parents, teachers or principals who seek to challenge the accuracy of PII as defined in 8 N.Y.C.R.R. Section 121.1(m) will do so by contacting the EA. If a correction to PII as defined in 8 N.Y.C.R.R. Section 121.1(m) is deemed necessary, the EA will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA's written request.

For security reasons, only pages 1-11 will be publicly posted

Secure Storage and Data Security	Please describe where PII as defined in 8 N.Y.C.R.R. Section 121.1(m) will be stored and the protections taken to ensure PII as defined in 8 N.Y.C.R.R. Section 121.1(m) will be protected: (check all that apply) ☐ Using a cloud or infrastructure owned and hosted by a third party. ☒ Using Contractor owned and hosted solution ☐ Other: Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data: All personnel are given several data security trainings each year, put on and mandated by Certiport's parent company, NCS Pearson, Inc. Certiport's processes are designed and developed to prevent the need for and sharing of student data and teacher and principal data, as defined by Education Law 2-d or 121, as well as education records (or personally identifiable information therefrom) as defined by FERPA
Encryption	Data will be encrypted while in motion and at rest.

CONTRACTOR	
[Signature]	Soo Kang (Nov 4, 2026 07:29:09 EST) HC
[Printed Name]	Soo Kang
[Title]	Executive Partner, Portfolio Management
Date:	11/04/2026

For security reasons, only pages 1-11 will be publicly posted

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.	Certiport's processes are designed and developed to prevent the need for and sharing of student data and teacher and principal data, as defined by Education Law 2-d or 121, as well as education records (or personally identifiable information therefrom) as defined by FERPA
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	All personally identifiable information is transmitted via TLS 1.2. All Student Data and Teacher or Principal Data including personally identifiable information, is stored in a secure SQL Server database, and is encrypted-at-rest. Access to the SQL Server database is restricted to database administrators and dev/QA personnel who must research issues and the resolution of the issues.
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.	Certiport, through its parent company, NCS Pearson, Inc., requires all employees (regardless of job function) to complete an annual Security and Data Privacy training course, which includes rules, laws and guidelines regarding access to, and handling of, student/user data.
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 employees and subcontractors are under confidentiality agreements. In addition Certiport and its subcontractors have technological and administrative controls designed to

		protect data and limit access to confidential information to only those individuals whose job functions require access. Reviews are conducted quarterly to ensure the only ones with access remain in employee job roles which continue to require the level of access.
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.	Certiport, through its parent company, NCS Pearson, Inc., has a centralized security team responsible for managing any data breaches. If Certiport experiences a data breach, the security team would immediately be notified. Notifications to the educational agency and other customers, as well as candidates, would be handled by the security team according to the requirements of the applicable laws and the contracts in place. All security breaches are handled on a case-by-case basis depending on the scope and nature of the breach as well as the requirements of laws and customers.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Certiport retains all data that an end user or an end user's legal guardian has consented for Certiport to retain and use and any and all data collected by Certiport during registration and administration of an examination of end users. This data is retained in individual user accounts which allow the end user to control and manage their certifications and allows Certiport to verify and validate certifications earned by end users.
7	Describe your secure destruction practices and how certification will be provided to the EA.	N/A
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	Certiport's processes and data security and privacy program are designed to comply with all applicable provisions of FERPA, COPPA, PPRA, IDEA, New York Education Law Section 2- d; and the

		Commissioner of Education's Regulations at 8 NYCRR Part 121 and to ensure that the EA is in compliance with said statutes, laws, and regulations.
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 importance to organizational objectives and the organization's risk strategy.	Contractor has an asset management team that accounts for all systems on Contractor's domain
	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.	**Yes**
	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.	**Yes**
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**Yes**
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk	**Yes**

Function	Category	Contractor Response
	tolerances, and assumptions are established and used to support operational risk decisions.	
	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are 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.	Yes
PROTECT (PR)	**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.	Yes
	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.	**Yes, every year this is reviewed and updated**
	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.	**All data is managed consistent with these areas**
	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.	Security policies have been created and maintained by our security teams
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	Yes
	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.	Yes
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood.	Yes, all anomalous activities are detected and reviewed

Function	Category	Contractor Response
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	Yes, all systems are monitored and reviewed frequently.
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	Yes, these policies are reviewed and maintained by our security teams.
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	Yes, these policies are reviewed and maintained by our security teams.
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	**Yes, if the need arose this would be done**
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	Yes, frequently
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	Yes, frequently
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	Yes, frequently
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	Yes, frequently
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	Yes, frequently
	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).	**Yes, if the need arose, this would be completed**