Exhibit 8635-E

PARENT BILL OF RIGHTS FOR STUDENT DATA PRIVACY AND SECURITY THIRD PARTY CONTRACTOR SUPPLEMENT

The NCS Pearson, Inc. has been engaged by Rockland Board of Cooperative Educational Services to provide services. In this capacity, the company may collect, process, manage, store or analyze student or teacher/principal personally identifiable information (PII).

The NCS Pearson, Inc. will provide Rockland BOCES with specific purpose for which PII will be used Q-global and Q-interactive clinical assessments.

The NCS Pearson, Inc. will ensure that subcontractors or others that the company shares PII will abide by data protection and security requirements of Rockland BOCES data privacy and security policy, and state and federal law and regulations as defined in the Data Privacy Contractor Agreement.

PII will be stored as defined in the Data Privacy Contractor Agreement.

Parents may challenge the accuracy of PII held by contacting

Rockland BOCES. Rockland BOCES will contact NCS Pearson, Inc..

The NCS Pearson, Inc. will take reasonable measures to ensure the confidentiality of PII by implementing the following :

- ***Password protections***
- ***Administrative procedures***
- ***Encryption while PII is in motion and at rest***
- ***Firewalls***

The NCS Pearson, Inc. agrees to be bound by the Rockland BOCES Parents' Bill of Rights and Data Privacy & Security Policy.

The contractor's agreement with the district begins on 09/01/22 and ends on 09/01/22. Once the contractor has completed its service to the district, records containing student PII will be returned as per the Data Privacy Contractor Agreement.

Name of contractor: NCS Pearson, Inc.

Name, Title: Randall T. Trask
Randall T. Trask (Aug 31, 2021 15:54 CDT)

Randall T. Trask

SVP

Date: 09/01/22

DATA PRIVACY AGREEMENT

ROCKLAND BOCES

and

NCS PEARSON, INC.

This Data Privacy Agreement ("DPA") is by and between the Rockland BOCES ("EA"), an Educational Agency, and NCS Pearson, Inc. ("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 September 1, 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 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**.

Contactor 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. As applicable, upon expiration or termination of the Service Agreement, Contractor shall transfer PII, in a format agreed to by the Parties to the EA.

(b) If applicable, once the transfer of PII has been accomplished in accordance with the EA's written election to do so, Contractor agrees to return or destroy all PII when the purpose that necessitated its receipt by Contractor has been completed. Thereafter, with regard to all PII (including without limitation, all hard copies, archived copies, electronic versions, electronic imaging of hard copies) as well as any and all PII maintained on behalf of Contractor in a secure data center and/or cloud-based facilities that remain in the possession of Contractor or its Subcontractors, Contractor shall ensure that PII is securely deleted and/or destroyed in a manner that does not allow it to be retrieved or retrievable, read or reconstructed. Hard copy media must be shredded or destroyed such that PII cannot be read or otherwise reconstructed, and electronic media must be cleared, purged, or destroyed such that the PII cannot be retrieved. Only the destruction of paper PII, and not redaction, will satisfy the requirements for data destruction. Redaction is specifically excluded as a means of data destruction.

(c) Contractor shall provide the EA with a written certification of the secure deletion and/or destruction of PII held by the Contractor or Subcontractors.

(d) 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:

Laura Davie
DPO
65 Parrott Road
West Nyack, NY 10997
ldavie@rboces.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 full 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.

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: NCS PEARSON, INC.**
BY:	BY: Randall T. Trask Randall T. Trask (Aug 31, 2021 15:54 CDT)
Name:	Name: Randall T. Trask
Title:	Title: SVP
Date:	Date: Aug 31, 2021

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

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any Commercial or Marketing purpose. PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.

2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency. This right may not apply to Parents of an Eligible Student.

3. State and federal laws such as Education Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, 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); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student's identifiable information.

4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.

5. A complete list of all student data elements collected by NYSED is available at www.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.

6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to Laura Davie, Rockland BOCES, 65 Parrott Rd, West Nyack, NY 10977; by email to ldavie@rboces.org or by telephone at 845-627-4822 (ii) Complaints may also be submitted to the NYS Education Department at www.nysed.gov/data-privacy-security/report-improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to privacy@nysed.gov; or by telephone at 518-474-0937.

7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.

8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.

9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

CONTRACTOR: NCS PEARSON, INC.	
Signature:	Randall T. Trask Randall T. Trask (Aug 31, 2021 15:54 CDT)
Printed Name:	Randall T. Trask
Title:	SVP
Date:	Aug 31, 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	**NCS Pearson, Inc.**
Description of the purpose(s) for which Contractor will receive/access PII	**Q-global and Q-interactive collect, process and store the data for administering, scoring, and reporting on clinical assessments.**
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 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) ☒ Using a cloud or infrastructure owned and hosted by a third party. ☐ Using Contractor owned and hosted solution ☒ Other: Pearson develops, maintains and supports Q-global and Q-interactive which are hosted at Amazon Web Services. Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data: Q-global and Q-interactive data are hosted at Amazon Web Service (AWS) Canada Central region in Montreal, QC, Canada. Some data within Q-global are also hosted at AWS Europe West 1 region in North Dublin, Ireland. Pearson, Q-global, and Q-interactive employ many administrative, physical, and technical safeguards to protect customer data. Administrative safeguards include Pearson's Information Security Management Strategy based on the ISO 27001 Framework with movement towards NIST Cybersecurity Framework alignment which includes security

	policies and standards, information security and data privacy training for staff, least use privileges, configuration management, and formal processes for request and approval of accounts. Physical controls include physical lock and key, badge access systems, locking equipment cages, security guards, dedicated alarm systems, visitor logs, CCTV and video recording. For data centers, individual access is authorized only by the data center manager and based upon the individual's role, responsibilities, and business need. There is a data center control log that must be signed upon entrance and exit, and individuals must always present their access badge and display it visibly. Authorized employees must escort authorized visitors such as vendors, contractors, or consultants always in the data center. Technical controls include firewalls, segregated virtual private clouds for products and environments, separated tiers for servers, data encryption for data at rest (AES 256) and in transit (TLS and HTTPS), role-based access and authentication, unique and complex authentication, secure coding practices, OS and application patching, and static and dynamic security scanning.
Encryption	Data will be encrypted while in motion and at rest.

CONTRACTOR: NCS PEARSON, INC.	
Signature:	Randall T. Trask Randall T. Trask (Aug 31, 2021 15:54 CDT)
Printed Name:	Randall T. Trask
Title:	SVP
Date:	Aug 31, 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.	Pearson, Q-global, and Q-interactive employ many administrative, physical, and technical safeguards to protect customer data.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	Administrative safeguards include Pearson's Information Security Management Strategy based on the ISO 27001 Framework with movement towards NIST Cybersecurity Framework alignment which includes security policies and standards, information security and data privacy training for staff, least use privileges, configuration management, and formal processes for request and approval of accounts.
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.	Physical controls include physical lock and key, badge access systems, locking equipment cages, security guards, dedicated alarm systems, visitor logs, CCTV and video recording. For data centers, individual access is authorized only by the data center manager and based upon the individual's role, responsibilities, and business need. There is a data center control log that must be signed upon entrance and exit, and individuals must always present their access badge and display it visibly. Authorized employees must escort authorized visitors such as vendors, contractors, or consultants always in the data center.
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.	Technical controls include firewalls, segregated virtual private clouds for products and environments, separated tiers for servers, data encryption for data at rest (AES 256) and in transit (TLS and HTTPS),

		role-based access and authentication, unique and complex authentication, secure coding practices, OS and application patching, and static and dynamic security scanning.
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.	Q-global and Q-interactive data are hosted at Amazon Web Service (AWS) Canada Central region in Montreal, QC, Canada. Some Q-global data are hosted at AWS Europe West 1 region in Ireland.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Pearson, Q-global, and Q-interactive employ many administrative, physical, and technical safeguards to protect customer data.
7	Describe your secure destruction practices and how certification will be provided to the EA.	Administrative safeguards include Pearson's Information Security Management Strategy based on the ISO 27001 Framework with movement towards NIST Cybersecurity Framework alignment which includes security policies and standards, information security and data privacy training for staff, least use privileges, configuration management, and formal processes for request and approval of accounts.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	Physical controls include physical lock and key, badge access systems, locking equipment cages, security guards, dedicated alarm systems, visitor logs, CCTV and video recording. For data centers, individual access is authorized only by the data center manager and based upon the individual's role, responsibilities, and business need. There is a data center control log that must be signed upon entrance and exit, and individuals must always present their access badge and display it visibly. Authorized employees must escort authorized visitors such as vendors, contractors, or consultants always in the data center.
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.	**See attached documents describing the Pearson Information Security Program and Pearson Information Security Controls which are NIST aligned:** **1) Pearson Information Security Controls - see attached Attachment A** **2) Pearson Clinical Assessments Information Security Program - see attached Attachment B**
	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.	
	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.	
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk 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.	

Function	Category	Contractor Response
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.	
	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.	
	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.	
	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.	
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	
	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.	
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood.	
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and	

Function	Category	Contractor Response
	maintained, to ensure response to detected cybersecurity incidents.	
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	
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.	
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	
	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).	

ATTACHMENT B

Pearson Clinical Assessments Information Security Program

PEARSON ASSESSMENTS

Information Security Office

2020.12.01 v1.8

Table of Contents

Information Security Program

Overview

Information Technology (IT) systems are trusted only when the data and information they contain are kept confidential and secure. And this can only happen when a comprehensive information security program governs its design, development, and delivery of the services they provide. Pearson takes the privacy and security of customer and company information seriously. To protect sensitive assessment data, such as test items and student confidential information, Pearson employs recognized industry standard security measures to safeguard the confidentiality, integrity, and availability of customer data and the services we provide.

Our information security policies and standards are based on the ISO/IEC 27001 information systems security framework, and we continue to work toward also aligning our program with the NIST catalogue of security controls. This evolving alignment with NIST reflects our ongoing commitment to ensure our information security program remains current and appropriate to address the evolving threats to information security and data privacy.

In support of this, Pearson's technology teams are encouraged to continually improve their skills and gain professional recognition for their mastery of them. To this end, the teams that support and maintain the systems that provide services to our customers collectively hold numerous professional certifications in the areas of AWS Architecture, AWS DevOps, AWS Development, Splunk Log Management, Jenkins Deployment, Java Development, Data Science Analytics, Information Security, Information Privacy, Project Management, and Agile Scrum Mastery, just to name a few. Because of our teams' well-established experience and credibility as technology professionals, our more senior level staff regularly sit on discussion panels and speak at local, regional, and national conferences.

System Security and Resiliency

In accordance with security best practices, multiple layers of security exist in the computing environment to reduce the risk of unauthorized exposure of customer data. These protections include not only preventive controls designed to stop security incidents from happening, but also detective controls to inform us in the unlikely event a security control failure occurs. Along with the resilient and reliable design of our assessment platform, Pearson leads the industry in its ability to protect against and mitigate the effects of distributed denial of service (DDoS) attacks.

Staff Training Requirements

When employees and staff augmentation resources begin working for Pearson, they must sign an acknowledgement of their obligation to adhere to the Pearson Global Information Security Policies and follow the company's implementation guidelines and standards. On an annual basis, members of the Pearson workforce must complete information security training that is designed to ensure they not only maintain awareness of their responsibility to protect customer and company information, but also to help ensure they are educated regarding changes in the ever-evolving information risk universe.

Need to Know and Least Privilege

Pearson provides access to systems based on *need to know* and in accordance with the *principle of least privilege.* If a workforce member does not have a business need for access, they do not get it. And where access is authorized, user accounts are assigned the minimum level of privilege necessary for their role.

These principles also extend into the assessment services we provide. Customer staff who have been assigned to administration roles in service solutions have the ability to place staff into specific roles, with privileges appropriate to them. In this way, administration of the assessment platform can conform to role-based access needs of each customer.

Entitlement Review

A review of users and the permissions assigned to them is performed periodically, as well as when staff change positions and employment statuses change. This helps to ensure on-going adherence to our commitment to grant access based on *need to know* and according to the *principle of least privilege*.

Data Classification

Pearson's Global Information Security Policies and Standards define a four-tier data classification level (DCL) scheme. DCL4, the highest classification tier, denotes data subject to data privacy regulation and requires the most stringent information security controls. Given the nature of the services we provide to customers, practically all of our systems are designed with the baseline assumption that the data it maintains and processes is DCL4.

Governance, Risk, and Compliance

Pearson’s executive management is committed to ensuring the customer and company data we hold is not only secure and confidential, but also meets applicable regulatory requirements. This requires ensuring appropriate governance over matters of information security risk and privacy compliance. To this end, Pearson Assessments has an established cadence for evaluating the risk landscape for ongoing compliance to internal and external security and privacy requirements. This includes an internal risk assessment process that evaluates the threat landscape and determines where new controls need to be put in place, as well as existing controls strengthened.

Audits

Annually, certain systems within our assessment platform undergo an external Service Organization Control 2 (SOC2) audit, adhering to the Association of Independent Certified Public Accountants (AICPA) Statement on Standards for Attestation Engagements No.18 (SSAE 18), the most recent version, which became effective May 1, 2017.

Whether performed internally by trained and experienced staff or externally by an independent third-party audit firm, if gaps or weaknesses in our security and privacy controls are identified, they are reported to the Pearson Assessments Information Security Office (AISO), who then works with business, legal compliance, and technical management to identify and implement appropriate remediation solutions.

Remediation

Remediation efforts focus on reducing risk to an acceptable level or eliminating it altogether. These projects are typically assigned a technical project manager (TPM), who works with the appropriate subject matter experts (SME) and stakeholders to develop a remediation plan, determine roles and responsibilities, establish target dates and milestones, and provide ongoing oversight throughout the life of the project. Relevant documentation is created and published internally by members of the project team, ensuring effective communication and appropriate visibility of remediation efforts and changes.

Corporate Governance

Pearson’s Global Corporate Information Security Office (CISO) defines, publishes, and socializes information security ISO-aligned policies and standards. The CISO has further defined organizational roles to carry out the information security mandate within each line of business (LOB). Through roles focused on the various aspects of information security, the policies and standards propagate to the individual business units that make up that region’s component of the LOB in which they operate. The Pearson Assessments LOB maintains a dedicated information security office team to support not only the adoption of Pearson’s Global Information Security Policy, but also to ensure customers’ specific information security requirements are met.

Security Incident Management & Response

Executive management supports a defined security incident management team with direct responsibilities for the management and response to security Incidents. Only authorized, trained personnel within this group are given responsibility for incident management and response.

Responsibilities and procedures are established and documented for the Incident Management Team. These include procedures for:

- monitoring, detecting, and reporting security events.
- assessment, classification, and decision on security events.
- response, escalation, recovery, and communication.
- for timely collection, protection and preservation of relevant system and application logs, and all other evidence pertaining to the incident in compliance with technical forensic needs and applicable legal requirements.

Security Incidents are categorized based upon the incident severity. Procedures exist and provide guidance on the proper handling of any potential incident, regardless of severity level. The severity levels range from Critical events with business disruption on a massive scale, to Low-severity events that are isolated to a small number of individuals, systems, or processes.

All communication on security Incidents, both internal and external are strictly controlled and only initiated by authorized staff, which is done in consultation with Pearson Legal and Pearson Corporate Affairs.

Regulatory Compliance

As with any company that operates in multiple countries, compliance to the laws of each jurisdiction play a central role in the definition of its policies, standards, and guidelines. Pearson takes this responsibility seriously, ensuring the security and privacy of customer data conforms not only to the contractual obligations of its customers, but also to the compliance requirements of the jurisdictions in which they operate.

To this end, Pearson Assessments maintains trained, qualified professionals whose responsibilities include staying abreast of applicable regulatory requirements. By the very nature of the services we provide, the privacy of student data sits at the top of our information security program’s list of high-value, critical information assets. As such, everything we do carries a measure of consideration for ensuring we meet the obligations of Federal, State and Provincial data privacy laws

Data Residency

Pearson respects the data privacy laws of the jurisdictions in which we do business. We recognize that data residency has become an important consideration when selecting a service provider who will handle confidential and sensitive information—particularly personal identity information. To this end, all of the data collected, stored, processed, maintained, and transmitted by Pearson Assessments' systems reside within the jurisdictions outlined in the governing customer contract. If the data is allowed to only reside and be transmitted within a certain country or jurisdiction, Pearson will work with our customers to identify an appropriate solution to meet data residency requirements. Our use of Amazon Web Services affords us the flexibility to limit where data is stored and the destinations to which it is transmitted.

Cyber-Attack and Exfiltration Defence

Pearson employs a number of different methods to mitigate the risk of unauthorized access to our systems:

- All data transmitted externally is encrypted.
- All item content payloads are encrypted end-to-end using AES encryption.
- All student/patient responses are encrypted using AES encryption, and use a key that is different from the key used to encrypt content payloads.
- Account and password controls meet accepted industry standards for length, complexity, re-use, expiration, and log-on retry lockout.
- Accounts are only given the least set of privileges needed to perform authorized activities.
- Anomaly detection built into the application allows Pearson engineers to detect unexpected or potentially harmful application behaviour in near-real-time.

Antivirus and Malware Controls

All workstations and servers on the internal Pearson network make use of installed antivirus and malware detection software. Malware definition updates occur automatically, ensuring all workstations in the Pearson network can detect and quarantine known malicious software. Additionally, the annual information security training mentioned above, includes modules to educate our workforce to such things as social engineering and phishing.

Windows servers, because of the virtually ubiquitous use across the globe and its foundational similarity to its desktop OS counterpart, employ anti-virus/anti-malware software—particularly for any servers that are directly accessible from the Internet.

The operating system that is most prevalent in the design and architecture of the systems providing our assessment services are variants of Linux (*e.g.,* Amazon Linux, CentOS, Ubuntu), which have been risk assessed in conjunction with system architecture.

The risk assessment determined that stability and performance of the Linux variants were at greater risk when anti-malware tools were deployed. For this reason, a defence-in-depth design that precludes direct Internet access to the servers in the cloud environment has been implemented, thus dramatically reducing the risk of malware infection compared to the risk of destabilizing and/or degrading the environment. We continually monitor the risk landscape for changes in technology and cyberattack vectors that would impact this risk decision.

Wireless Network Security

Pearson's wireless network requires users to be members of Pearson's Active Directory trusted domain to ensure only authorized users can connect to the internal network. All transmissions over the wireless network make use of strong encryption. Further, since our assessment platforms exist 100% in the cloud, the Pearson wireless network does not have a direct connection to them.

System Maintenance

As with all information technology solutions, patches, updates, and fixes to unexpected events need to be deployed from time to time. Pearson establishes regular maintenance windows and coordinates with customers as needed to ensure minimal interruption to assessment services. Our goal is to make sure customers know in advance about any update or system downtime that may be necessary.

Vulnerability Management & Patching

Patches are released periodically by the manufacturers of Pearson's underlying system components, devices, platforms, and applications. Each patch undergoes an assessment to determine applicability, risk, and whether or not mitigating controls already exist.

If the assessment determines a patch to be necessary, it is applied in a test environment where it is regression tested to verify the patch works and does not negatively impact the assessment platform. Once regression testing completes, user acceptance testing (UAT) is performed to confirm the platform is fully operational. If the patch passes UAT, then we send notification, as applicable, to affected customers and release the patch into the production environment through a standardized change control process.

Change Management

Our change management processes are designed to reduce the risk of service interruption and degraded performance, as well as to ensure all changes made to production system are authorized. Rigorous adherence to change controls throughout the system development lifecycle (SDLC) works to ensure successful implementation on the first attempt.

The process includes:

- acknowledgement and record of changes
- assessment of the impact to the costs, benefits, and risks of proposed changes
- management approval
- management and coordination of implementation
- closure review

Web Components and Transmission

Pearson employs HTTPS, an encrypted method of passing data over the Internet via web-based systems. Transport Layer Security (TLS) works with HTTPS to ensure the data is encrypted as it passes from our servers to the clients. Web-based services and application layer interface (API) calls use industry standard representational state transfer (REST) architecture to appropriately constrain and control data as it passes between components and across connections.

File Transmission

Pearson's assessment platforms provide for the ability to transfer student data to customer-authorized destinations via multiple methods, based on the needs of the customer. Such methods of file transfer include:

- Synchronous:
    - Pearson's cloud-based solution leverages customers' ability to establish connections directly to the cloud storage repositories where extracts of the data can be placed. Customers are issued authentication and access credentials, as well as instructions describing how to use this solution.
    - Secure FTP can be used, as well, enabling customers to pull data from SFTP servers over an SSH connection using commonly available SFTP client software.
- Asynchronous:
    - Based on the needs of customers, Pearson is often able to meet specific data transfer requirements through a collaborative effort to define and implement a suitable solution.

System Logging

Pearson’s assessment platforms possess extensive logging and monitoring capabilities. Some logs directly feed real-time monitoring systems and dashboards, while other logs facilitate troubleshooting and forensic analysis. Examples of logged events include, but are not limited to:

- User provisioning and access level assignment
- Logon and logoff success and failure events, along with date and time
- Database access
- Transmission of data and files
- System errors, aborts, and other events to enable detection of anomalous behaviours

System Monitoring

Although we constantly monitor for anomalous system behaviour, special care is taken during student testing cycles to provide the highest possible levels of availability and performance. Our monitors watch for anomalous activity throughout the entire system, not just at the application or network layers. If suspicious activity shows up on our systems, our system triggers alerts to our technical staff for investigation and handling.

In addition to overall, system-wide monitoring for suspicious and anomalous system activity, we also make sure our systems remain at current patch levels. We use a suite of tools to scan for vulnerabilities at the network, operating system, platform, and application layers.

Service Delivery Analytics

Our assessment solutions include extensive logging features, which enable detailed performance and test activity analytics, particularly as it regards such things as the type of browser, IP addresses, operating system type, and usage statistics. Pearson maintains a dedicated system status dashboard for each program detailing real-time status for all key technology services involved in the given assessment delivery chain. Industry standard web analytic services collect statistics to provide a comprehensive view into technology and platform usage.

Dependable, Scalable, and Resilient Architecture

Overview

A successful testing experience for each student requires technology that is not only secure, but also dependable, scalable, and resilient. Pearson's assessment platforms meet these requirements through the use of cloud-based hosting infrastructure, system isolation, and elastic compute power. We augment this with careful 24x7 tracking of system performance metrics.

We deliver consistent testing and assessment performance, even when subject to widely fluctuating demands on our environment, where the load can swing rapidly from periods of low demand to high. Our technology and architecture allow us to rapidly adjust to sharp changes in system demand, increasing capacity at the time demand occurs, instead of waiting to perform scale-up operations during off-hours. Because of this, students and teaching staff can focus on learning and teaching, instead of on the technology that enables them.

Cloud-based Architecture

Hosting our solutions in a virtual private cloud (VPC) affords our customers with the quality, security and scalability they expect. We have designed our platforms to be cloud-native and dynamically scalable.

Security Features

Advanced security measures, such as at-rest and in-transit data encryption, IP-based and identity-aware network filtering, web application firewall capability, industry standard network access controls and authentication processes, increased flexibility to provide data access to authorized users...in short, customer confidential and personal identity information, along with test items, student/patient responses, and other data considered sensitive or subject to regulatory compliance are protected with the most up to date technologies available. This is in addition to ensuring the data is encrypted from end to end.

Scalability

Virtually unlimited scalability gives Pearson the ability to quickly meet the resource demands during peak testing volumes, which ensures consistent performance for students and teachers when they need it most.

Resiliency

Redundancy and fault-tolerance form the foundation of all our assessment platform components. If one component of the system experiences problems, the platform shifts traffic to other servers in configured availability zones. Availability zones can be equated to datacentres, which are geographically separated from one another. This geographic separation is often referred to in the industry as the “air gap.” This sustains not just high availability through automatic load balancing, but also high resiliency against disaster events. And, equally important, ensures a consistent performance experience. This approach allows us to provide secure, high quality services even under the most demanding workloads and threat conditions.

Auto-scaling

In addition to the use of availability zones, we build auto-scaling capabilities into each customer critical system we provide. Based on real-time load and incoming monitoring data, compute capacity dynamically increases to handle whatever the processing load demands. When auto-scaling kicks in, new servers get spun up and undergo a series of automated quality checks before coming fully online to serve customer traffic. In this way, the infrastructure dynamically scales to give our customers stable, reliable service.

Network Control

Pearson’s approach to standing up and provisioning our systems in the cloud affords us the ability to maintain full control of incoming and outgoing data access traffic on a per-system basis. Instead of relying only on a centralized firewall perimeter, as is typical in brick-and-mortar datacentres, our cloud-based architecture gives us increased cybersecurity protection through more granular control over what traffic is allowed in and out of the cloud. The VPCs that host our systems are isolated from other public cloud services, as well as from the public Internet. Because of these isolation and network segmentation options, customer data gains an inherently higher level of protection and isolation.

Accessibility

VPCs are, by definition, hosted in an Internet-accessible cloud environment, which negates the need for private extranet links to be created between Pearson and its customers. This allows us and our customers to avoid the costs associated with specialized network services and connections.

Open Source Tech Stack

We use an open source technology stack, which dramatically reduces software costs compared to our competition. It gives Pearson the ability to use the most robust, affordable, and customizable solutions available in the technology market today.

Disaster Recovery and Resiliency

Disaster declaration is governed by the decisions of the Disaster Response and Recovery Team, which is formed at the outset of any system-wide or company-wide event that disrupts service and thereby threatens the confidentiality, integrity, or availability of valuable information assets. Pearson's Disaster Recovery and Incident Management policies provide high-level guidance regarding the classification of events and defines four severity categories, as follows:

- Critical – Level 1 Events that have the potential to disrupt business on a massive scale, or have material legal, strategic, operational or financial implications. All suspected or known personal data breaches must be classified as Critical – Level 1.
- High – Level 2 Events that have the potential to disrupt business on a large scale, or have significant legal, contractual, or financial implications.
- Moderate – Level 3 Events likely to cause service disruptions to isolated groupings of systems or processes and have limited legal, strategic, operational or financial implications.
- Low – Level 4 Events isolated to a small number of individuals, computers or processes that are unlikely to have any meaningful impact to the organization.

With regard Disaster Resiliency, Pearson replicates all data, systems, and components across multiple availability zones to maintain physically redundant and geographically-dispersed replicas of the production environment. This dramatically reduces the risk of experiencing service-impacting events associated with such events as fire, flood, earthquake, and other similar events. The use of VPCs, elastic computing, and the services offered our cloud provider, allows for physical and logical redundancy that is unmatched in the industry. The disaster recovery procedures, inclusive of automated services and manual actions, exist in disaster recovery runbooks. This documentation is version-controlled and kept up to date by trained Pearson staff.

Data Backup

In traditional backup methods, a full backup of the data is taken only when system loads are low, such as during the night on weekends. During the week, the traditional method typically only backups the data that changed each day, thereby requiring longer and more complex restore processes.

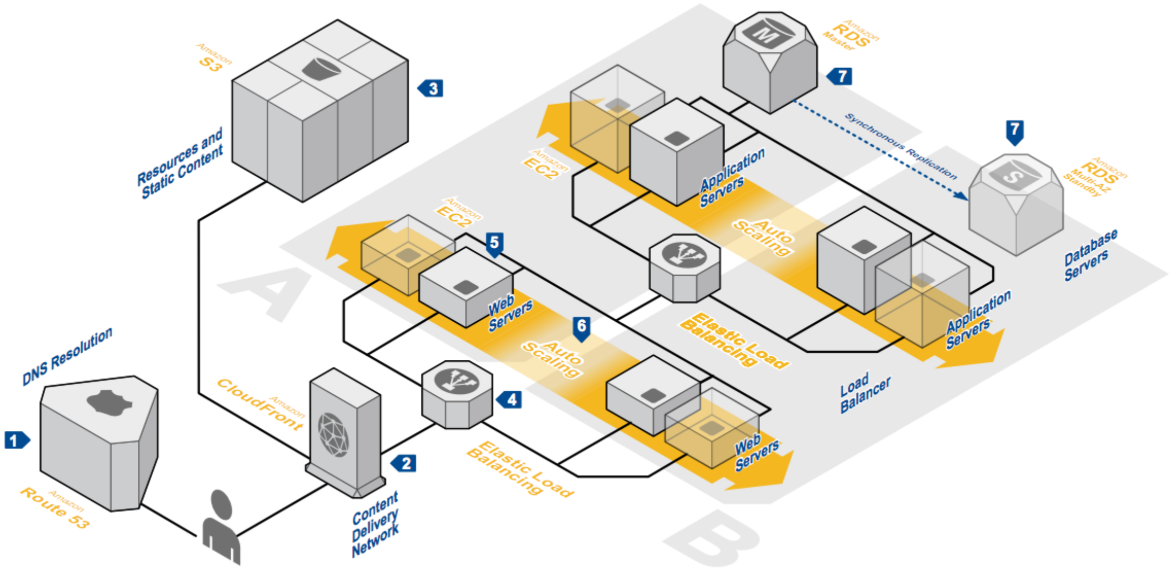
Pearson’s backup method replicates data securely on a near-real-time basis, which means we maintain a full backup of customer data at all times, enabling a more robust ability to recover or restore data to the point in time closest to the event that is possible.

Automated systems monitor production data replication services, and any failure or delay in backup or replication operations will generate an alert to Pearson’s on-call staff. In this way, we are able to provide high assurance to our customers that their data remains safe, backed up, and secure.

Pearson’s data backup operations use Transport Layer Security (TLS) encryption when transmitting the data both internally and externally. And the backed up data at rest (called “snapshots”) enjoys the protection afforded by the Advanced Encryption Standard (AES) encryption algorithm, the industry’s strongest encryption, and does so at 256-bit strength. These snapshots are taken at intervals defined based on risk and will vary among systems, but at a minimum occur daily.

Logical Architecture Diagram

The diagram below depicts a typical network architecture for our cloud-based solutions.



Reference: Amazon Web Services (http://media.amazonwebservices.com/architecturecenter/AWS_ac_ra_web_01.pdf)

ATTACHMENT A

Pearson

Information Security Controls

Summary of Information Security Controls: Alignment w/NIST SP800-53r4

PEARSON SCHOOL ASSESSMENTS

Assessments Information Security Office

William L. Wells, CISSP, CISA, CISM, CRISC, CIPP/IT

2021.08.02

Table of Contents

Information Security Controls: Alignment w/NIST SP800-53r4

Overview

This document provides an overview of the information security controls and environment for Pearson's assessments systems in the context of their alignment to the National Institute of Standards and Technology's (NIST) Special Publication 800-53 revision 4 (SP800-53r4).

Background

Pearson Assessment's information security program is governed by Pearson's Corporate Information Security Office (CISO) and supported directly by the Pearson School Assessments Information Security Office (AISO). The information security program is currently aligned to the ISO/IEC 27001 information security standards, with an evolving and maturing focus to align it more closely with the NIST SP800-53r4 catalogue of controls.

The intent of this document is to provide an overview of our information security controls as they relate to the SP800-53r4 catalogue and the 18 families of security controls. Below is a table that lists the families and their two-letter identifier.

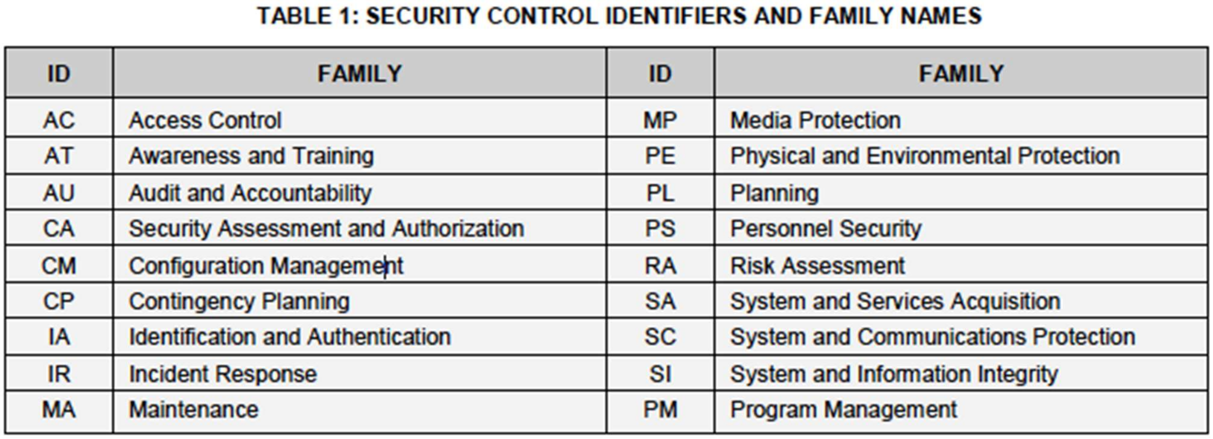


TABLE 1: SECURITY CONTROL IDENTIFIERS AND FAMILY NAMES

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

The 18 Families of Information Security Controls

AC – Access Control

As established by policy, access to information assets is strictly controlled. Users are granted access to systems and data based on their business need and limited to the least level of privilege necessary to perform their job functions. Prior to granting access, approval must be obtained from appropriate system and data owners. Access is enforced at multiple levels of the technology stack, including network, operating system, application, and database layers, as well as points of integration between applications. Information flow control is made possible through software-defined networking controls available to our applications hosted in the Amazon Web Services cloud. Segregation of duties is implemented through the use of role-based access and unique user IDs. And if a user exceeds the allowed number of logon attempts, the account is automatically locked.

AT – Awareness and Training

As a matter of policy, all members of the workforce are required to complete annual information security and data privacy training. In addition to the training sponsored by the CISO, additional training is provided on focused topics as needed. New workforce members are required to complete the information security and data privacy training before being given access to confidential information, which includes, Pearson proprietary information and customer data.

AU – Audit and Accountability

All systems are required, by established policy, to implement audit logging with a defined set of auditable events. The logging policy prohibits the inclusion of personal identity information (PII) in audit logs, requiring tokenization or other equally effective methods of obfuscation for those occasions when business need demands its inclusion. Audit logs entries are time- and date-stamped using the system date and time as synchronized with network time protocol (NTP) servers and they are secured against tampering and repudiation. As a matter of policy, information security-related logs are kept for 1 year, unless dictated otherwise by customer contract or regulatory requirements—HIPAA, for example.

CA – Security Assessment and Authorization

Established policy requires risk assessments to be performed at least annually. The risk assessments are aligned to the NIST SP800-53r4 catalogue of controls and are intended to identify gaps or weaknesses in the information security controls required. Additionally, certain systems are subject to annual Service Organization Control 2 (SOC 2) audits performed by external auditors. In addition to risk assessments and audits, certain key systems are also subjected to annual penetration testing. Findings from the assessments, audits, and penetration tests, if any, are reviewed by appropriate subject matter experts to confirm the gap or weakness. Once confirmed, the risk is quantified and presented to management stakeholders for dispositioning. As a general statement, any findings rated “Medium” or higher are assigned target dates for remediation and resources are assigned accordingly.

CM – Configuration Management

Our approach to configuration management leverages features and functions available on the AWS cloud hosting platform. Server instances are built using standardized base images that contain the operating system and other platform-specific installations. In this manner, a baseline configuration is in place that is maintained and subject to version controls. Change control is implemented via a release engineering pipeline that goes through multiple test cycles as new code moves through the development, test, staging, user acceptance…and other environments before being approved to be pushed to the production environment. Changes to production must be approved and are deployed by the release engineering team.

CP – Contingency Planning

Our contingency planning for systems hosted in the AWS cloud reflects the enhanced resiliency inherent to the hosting platform. In a traditional brick-and-mortar datacenter, solutions that provide fault-tolerance and high availability are often cost prohibitive. By contrast, such features in the AWS cloud are provided as standard functionality, without the prohibitively high cost of standing up fault-tolerant solutions (read: buying duplicate hardware, installing and maintaining it, facilities costs…and so on). As a result, are systems are *disaster resilient*.

Our systems have been architected to distribute load across multiple physical datacenters. Should any one physical datacenter go down, load shifts to the other datacenter, which is positioned to be geographically distant from the other. As load increases, compute resources are automatically scaled up to meet the increased demand, thereby having minimal to no impact on the end users. Daily snapshots and weekly full backups are taken, which enables our ability to meet SLA-defined response time objectives (RTO) and recovery point objectives (RPO).

IA – Identification and Authentication

Established, documented policy requires users to be uniquely identified and that systems authenticate users before allowing access. Upon user ID assignment and provisioning, users are required to set their password during initial sign-on. The password must meet defined complexity and strength requirements. Passwords are stored as one-way, irreversibly encrypted (hashed) values. Where risk and/or business need dictates, workforce users are required to setup and use multi-factor identification.

IR – Incident Response

Defined incident response processes exist, including defined roles, workflows, and actions for responding and gathering relevant forensic information. All workforce members are provided training on their responsibility to promptly report known or suspected information security violations. The process pulls in a multi-disciplinary core team of experts to facilitate, manage, and coordinate all activities associated with the response effort. This core team is comprised of technical subject matter experts, business stakeholders, legal counsel, and information security. Other specialists are pulled in as needs of the incident dictate. The response process, though not a single-threaded process, in general flows as follows:

- Notification/Detection
- AISO Triage & Confirmation
- IR Core Team Formed
- Scope Determined
- Remediation
- Notification
- Post-Incident Review

MA – Maintenance

Information technology hardware maintenance is the purview of AWS, our cloud services provider. AWS holds multiple security certifications, a list of which can be found here: http://aws.amazon.com/compliance/programs.

Application maintenance varies by application, and all such changes are captured through change management processes. Change management verifies approvals have been obtained and all tests have been completed.

For those rare occasions requiring vendor-provided maintenance or support of the applications and underlying platforms, the changes are included in established change management processes. Any tools or devices brought on-site are vetted for appropriate security controls and are not allowed to connect to the internal network.

MP – Media Protection

As a matter of policy, media containing confidential information must be encrypted and access to the media restricted to authorized personnel. Media that is transported must be encrypted. Where encryption is not feasible/practical, the media must only be transferred by an authorized Pearson employee; or by an approved commercial courier that assures complete, documented chain of custody during the entire transportation process.

As a matter of policy, media sanitization is required prior to the transfer of ownership, discarding, scrapping, or repurposing. Sanitization methods must make the data unrecoverable by any means.

PE – Physical and Environmental Protection

Physical and environmental protections are, in large measure, the purview of our hosting services provider, AWS. Since the systems are hosted in the AWS cloud, no information technology equipment that is critical to the operation of our applications are hosted outside of AWS.

AWS datacenters are hosted in secure, undisclosed locations. More information about AWS security certifications and compliance can be found at: http://aws.amazon.com/compliance/programs and https://aws.amazon.com/compliance/data-center/data-centers/.

Regarding Pearson facilities, access is controlled by security guards at the main entrances and/or proximity ID badges. Visitors are required to sign-in, provide a picture ID to verify identity, and are escorted at all times by Pearson personnel. Video cameras monitor secure areas of the facility, in addition to entrance/exit points to the facilities.

PL – Planning

Information security planning is embodied in Pearson's Information *Security Management and Governance Policy*, which, among many other things, requires system architecture standards; security requirements definition activities on projects; policy documentation creation, maintenance, and dissemination; and a process for handling exceptions to security requirements for those situations where it is not feasible or practical to implement them. Security exceptions are reviewed and, based on risk, dispositioned by senior leadership.

PS – Personnel Security

Prior to being hired or otherwise engaged as contractors, personnel must submit to a criminal background check, in addition to rigorous interview- and credentials-based review. Upon termination, access to systems is promptly removed. Where members of the workforce change positions and job responsibilities, access and permissions are adjusted accordingly. All employees are required to sign confidentiality agreements prior to their first day of employment.

RA – Risk Assessment

Consistent with Pearson's information security policies, internal risk assessments are performed at least annually on key/critical systems. In addition, external Service

Organization Controls 2 (SOC 2) audits are conducted annually on certain key/critical systems. Vulnerability scanning occurs on multiple levels of the technology stack, including dynamic application security testing (DAST), static application security testing (SAST), platform vulnerability scanning, and specialized security analysis and review based on business need and identified potential risk.

SA – System and Services Acquisition

Policies and supporting processes are in place for ensuring security capabilities within acquired systems and services. New vendors must be on-boarded as an approved supplier and all are required to complete a security review process, as well as agree to data privacy protections. An extensive NIST-aligned questionnaire is used as a method of collecting detailed information security controls information. The questionnaires are reviewed, risks identified and communicated to appropriate leadership for dispositioning.

Software development follows an Agile-based system development lifecycle (SDLC) and a similar rigor is in place regarding infrastructure services and support. A change management process is in place that requires all changes to be reviewed, tested, and approved prior to publishing to production environments. As a general principle, we adhere to AWS best practices and guidelines, ensuring our implementation of AWS cloud services is consistent with industry-recognized standards of security management and data privacy configurations.

Our development and infrastructure teams collectively hold over 130 professional certifications in the areas of AWS Architecture, AWS DevOps, AWS Development, Splunk Log Management, Jenkins Deployment, Java Development, Data Science Analytics, Information Security, Information Privacy, Project Management, and Agile Scrum Mastery. Because of our technical teams' well-established experience and credibility as technology professionals, our more senior level technology and security staff regularly sit on discussion panels and speak at local, regional, and national conferences.

SC – System and Communications Protection

One of the many benefits of using cloud-based hosting services is the set of technical, physical, and administrative protections available to mitigate risks associated with distributed denial of service (DDoS) attacks and other similar attacks designed to disrupt service and violate system integrity. Pearson uses AWS Shield and Shield Advanced to protect against such attacks. The software defined network capabilities of AWS provide the ability to define system boundaries at a more granular level than can often be achieved in traditional brick-and-mortar datacenters. All transmissions over internal and external networks are encrypted using AES encryption. Both network-level IP/Port restrictions and identity-based access controls are used to deny unauthorized traffic to confidential data and information. Cryptographic keys are managed using

AWS's key management service (KMS), which ensures the keys are secure against unauthorized access. In short, information security controls are implemented at multiple levels of the technology stack, ensuring the security of systems and communications.

SI – System and Information Integrity

Our information systems are required to include dynamic and static vulnerability scanning of application code. Also required, is host-based scanning of the environment where the applications are running. Further, we perform vulnerability scans of open source software (OSS). Annual penetration tests are performed to ensure our systems remain hardened and resilient against cyberattacks. And as noted previously, these are in addition to security features and configuration options that are employed at multiple levels of the technology stack.

PM – Program Management

Management of the information security program is a collaborative effort between the Pearson Corporate Information Security Office (CISO), the Assessments Information Security Office (AISO), technical subject matter experts across a litany of professional disciplines, and business management and stakeholders.

An initiative began in 2019 to further align our ISO/IEC-aligned security controls framework with the NIST information security catalogue of controls (SP800-53r4). This decision was made to remain current with industry information security best practices in the markets we serve.

Our AISO organization manages the day-to-day functions and operations of the information security function within the business unit and leverages the tools, technologies, and methods promulgated by Pearson's CISO. Part of this includes participating in and interacting with information security groups and associations, locally, regionally, nationally, and globally.

The AISO also ensures focused and line-of-business-specific security and data privacy training is provided to the workforce to ensure local regulatory requirements of the jurisdictions in which we operate are communicated appropriately. Further, topics of security training are created to address the security requirements set forth in contracts—ensuring specific customer requirements are included in employee training.

The program is reviewed continuously. Strategic planning and oversight are integrated into business-as-usual processes to ensure all aspects of information security program management are addressed in a considered, appropriately comprehensive manner. Policies and standards are reviewed at least annually and updated as needed, based on changes and evolutions in the cybersecurity and threat landscape.

287118_NY Rockland BOCES_NCS Pearson_DPA

Final Audit Report 2021-08-31

Created:	2021-08-31
By:	Patricia Leighton (patricia.leighton@moraeglobal.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAA2cbflQH2M4oHNBBPFPDIuarklhuw_vP1

"287118_NY Rockland BOCES_NCS Pearson_DPA" History

Document created by Patricia Leighton (patricia.leighton@moraeglobal.com)

2021-08-31 - 8:24:52 PM GMT- IP address: 99.42.243.124

Document emailed to Randall T. Trask (randall.trask@pearson.com) for signature

2021-08-31 - 8:28:05 PM GMT

Email viewed by Randall T. Trask (randall.trask@pearson.com)

2021-08-31 - 8:54:02 PM GMT- IP address: 104.47.56.126

Document e-signed by Randall T. Trask (randall.trask@pearson.com)

Signature Date: 2021-08-31 - 8:54:41 PM GMT - Time Source: server- IP address: 66.242.90.244

Agreement completed.

2021-08-31 - 8:54:41 PM GMT