Address: 355 Harlem Rd

West Seneca, NY 14224

Address: 2510 N Dodge St Iowa City, IA

Date: 9/8/2023

EXHIBIT D

DATA SHARING AND CONFIDENTIALITY AGREEMENT

INCLUDING
PARENTS BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY
AND
SUPPLEMENTAL INFORMATION ABOUT THE MLSA

1. **Purpose**

(a) This Exhibit supplements the Master License and Service Agreement ("MLSA") to which it is attached, to ensure that the MLSA conforms to the requirements of New York State Education Law Section 2-d and any implementing Regulations of the Commissioner of Education (collectively referred to as "Section 2-d"). This Exhibit consists of the terms of this Data Sharing and Confidentiality Agreement, a copy of Erie 1 BOCES' Parents Bill of Rights for Data Security and Privacy signed by the Vendor, and the Supplemental Information about the MLSA that is required to be posted on Erie 1 BOCES' website.

(b) To the extent that any terms contained within the MLSA, or any terms contained within any other Exhibits attached to and made a part of the MLSA, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect. In the event that Vendor has online or written Terms of Service ("TOS") that would otherwise be applicable to its customers or users of its Product that is the subject of the MLSA, to the extent that any term of the TOS conflicts with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect.

2. **Definitions**

Any capitalized term used within this Exhibit that is also found in the MLSA will have the same definition as contained within the MLSA.

In addition, as used in this Exhibit:

(a) "Student Data" means personally identifiable information, as defined in Section 2-d, from student records that Vendor receives from a Participating Educational Agency pursuant to the MLSA.

(b) "Teacher or Principal Data" means personally identifiable information relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of New York Education Law Sections 3012-c or 3012-d, that Vendor receives from a Participating Educational Agency pursuant to the MLSA.

(c) "Protected Data" means Student Data and/or Teacher or Principal Data to the extent applicable to Vendor's Product.

(d) "Participating Educational Agency" means a school district within New York State that purchases certain shared instructional technology services and software through a Cooperative Educational Services Agreement with a BOCES, and as a result is licensed to use Vendor's Product pursuant to the terms of the MLSA. For purposes of this Exhibit, the term also includes Erie 1 BOCES or another BOCES that is licensed to use Vendor's Product pursuant to the MLSA to support its own educational programs or operations.

3. **Confidentiality of Protected Data**

(a) Vendor acknowledges that the Protected Data it receives pursuant to the MLSA may originate from several Participating Educational Agencies located across New York State, and that this Protected Data belongs to and is owned by the Participating Educational Agency from which it originates.

(b) Vendor will maintain the confidentiality of the Protected Data it receives in accordance with federal and state law (including but not limited to Section 2-d) and Erie 1 BOCES's policy on data security and privacy. Vendor acknowledges that Erie 1 BOCES is obligated under Section 2-d to adopt a policy on data security and privacy.. Erie 1 BOCES will provide Vendor with a copy of its policy. Vendor and Erie 1 BOCES agree to engage in good faith negotiations to modify this Data Sharing Agreement to the extent necessary to ensure Vendor's continued compliance with Section 2-d.

4. **Data Security and Privacy Plan**

Vendor agrees that it will protect the confidentiality, privacy and security of the Protected Data received from Participating Educational Agencies in accordance with Erie 1 BOCES' Parents Bill of Rights for Data Privacy and Security, a copy of which has been signed by the Vendor and is set forth below.

Additional elements of Vendor's Data Security and Privacy Plan are as follows:

(a) In order to implement all state, federal, and local data security and privacy requirements, including those contained within this Data Sharing and Confidentiality Agreement, consistent with Erie 1 BOCES' data security and privacy policy, Vendor will: Review its data security and privacy policy and practices to ensure that they are in conformance with all applicable federal, state, and local laws and the terms of this Data Sharing and Confidentiality Agreement. In the event Vendor's policy and practices are not in conformance, the Vendor will implement commercially reasonable efforts to ensure such compliance.

(b) In order to protect the security, confidentiality and integrity of the Protected Data that it receives under the MLSA, Vendor will have the following reasonable administrative, technical, operational and physical safeguards and practices in place throughout the term of the MLSA: The security and privacy plan is provided separately as "Pearson Clinical Assessments Information Security Controls Alignment w NIST 20210921"
[Insert here – also provide a copy of Data Security and Privacy Plan]

(c) Vendor will comply with all obligations set forth in Erie 1 BOCES' "Supplemental Information about the MLSA" below.

(d) For any of its officers or employees (or officers or employees of any of its subcontractors or assignees) who have access to Protected Data, Vendor has provided or will provide training on the federal and state laws governing confidentiality of such data prior to their receiving access, as follows: Annually, Vendor will require that all of its employees (or officers or employees of any of its subcontractors or assignees) undergo data security and privacy training to ensure that these individuals are aware of and familiar with all applicable data security and privacy laws.

(e) Vendor [*check one*] may utilize sub-contractors for the purpose of fulfilling one or more of its obligations under the MLSA. In the event that Vendor engages any subcontractors, assignees, or other authorized agents to perform its obligations under the MLSA, it will require such subcontractors, assignees, or other authorized agents to execute written agreements as more fully described in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

(f) Vendor will manage data security and privacy incidents that implicate Protected Data, including identifying breaches and unauthorized disclosures, and Vendor will provide prompt notification of any breaches or unauthorized disclosures of Protected Data in accordance with Section 6 of this Data Sharing and Confidentiality Agreement.

(g) Vendor will implement procedures for the return, transition, deletion and/or destruction of Protected Data at such time that the MLSA is terminated or expires, as more fully described in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

5. **Additional Statutory and Regulatory Obligations**

Vendor acknowledges that it has the following additional obligations with respect to any Protected Data received from Participating Educational Agencies, and that any failure to fulfill one or more of these statutory or regulatory obligations shall be a breach of the MLSA and the terms of this Data Sharing and Confidentiality Agreement:

(a) Limit internal access to education records to those individuals that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA).

(b) Limit internal access to Protected Data to only those employees or subcontractors that need access in order to assist Vendor in fulfilling one or more of its obligations under the MLSA.

(c) Not use education records for any purposes other than those explicitly authorized in this Data Sharing and Confidentiality Agreement.

(d) Not disclose any personally identifiable information to any other party, except for authorized representatives of Vendor using the information to carry out Vendor's obligations under the MLSA, unless:

(i) the parent or eligible student has provided prior written consent; or
(ii) the disclosure is required by statute or court order and notice of the disclosure is provided to Participating Educational Agency no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order.

(e) Maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of personally identifiable student information in its custody;

(f) Use encryption technology that complies with Section 2-d, as more fully set forth in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

(g) Provide notification to Erie 1 BOCES (and Participating Educational Agencies, to the extent required by, and in accordance with, Section 6 of this Data Sharing and Confidentiality Agreement) of any breach of security resulting in an unauthorized release of Protected Data by Vendor or its assignees or subcontractors in violation of state or federal law or other obligations relating to data privacy and security contained herein.

(h) Promptly reimburse Erie 1 BOCES, another BOCES, or a Participating School District for the full cost of notification, in the event they are required under Section 2-d to notify affected parents, students, teachers or principals of a breach or unauthorized release of Protected Data attributed to Vendor or its subcontractors or assignees.

6. **Notification of Breach and Unauthorized Release**

(a) Vendor shall promptly notify Erie 1 BOCES of any breach or unauthorized release of Protected Data in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after Vendor has discovered or been informed of the breach or unauthorized release.

(b) Vendor will provide such notification to Erie 1 BOCES by contacting Michelle Okal-Frink directly by email at mokal@e1b.org, or by calling (716) 821-7200 (office) or (716) 374-5460 (cell).

(c) Vendor will cooperate with Erie 1 BOCES and provide as much information as possible directly to Michelle Okal-Frink or her designee about the incident, including but not limited to: a description of the incident, the date of the incident, the date Vendor discovered or was informed of the incident, a description of the types of personally identifiable information involved, an estimate of the number of records affected, the Participating Educational Agencies affected, what the Vendor has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of Protected Data, and contact information for Vendor representatives who can assist affected individuals that may have additional questions.

(d) Vendor acknowledges that upon initial notification from Vendor, Erie 1 BOCES, as the educational agency with which Vendor contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department ("CPO"). Vendor shall not provide this notification to the CPO directly. In the event the CPO contacts Vendor directly or requests more information from Vendor regarding the incident after having been

initially informed of the incident by Erie 1 BOCES, Vendor will promptly inform Michelle Okal-Frink or her designees.

(e) Vendor will consult directly with Michelle Okal-Frink or her designees prior to providing any further notice of the incident (written or otherwise) directly to any other BOCES or Regional Information Center, or any affected Participating Educational Agency.

EXHIBIT D (CONTINUED)

PARENTS BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

Erie 1 BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law § 2-d, the BOCES wishes to inform the community of the following:

(1) A student's personally identifiable information cannot be sold or released for any commercial purposes.

(2) Parents have the right to inspect and review the complete contents of their child's education record.

(3) State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.

(4) A complete list of all student data elements collected by the State is available for public review at **http://www.nysed.gov/data-privacy-security/student-data-inventory**, or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

(5) Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be submitted using the form available at the following website **http://www.nysed.gov/data-privacy-security/report-improper-disclosure**.

BY THE VENDOR:

DocuSigned by:
Trent Workman
4FAB8B1D28F9446...

Signature

Trent Workman

Printed Name

SVP, Pearson School Assessment

Title

9/8/2023

Date

EXHIBIT D (CONTINUED)

SUPPLEMENTAL INFORMATION

ABOUT THE MASTER LICENSE AND SERVICE AGREEMENT
BETWEEN
ERIE 1 BOCES AND NCS PEARSON, INC

Erie 1 BOCES has entered into a Master License and Service Agreement ("MLSA") NCS Pearson, Inc. which governs the availability to Participating Educational Agencies of the following Product(s):

[aimswebPlus, WriteToLearn, and SSIS Social-Emotional Learning Edition on Review360]

Pursuant to the MLSA, Participating Educational Agencies may provide to Vendor, and Vendor will receive, personally identifiable information about students, or teachers and principals, that is protected by Section 2-d of the New York State Education Law ("Protected Data").

Exclusive Purpose for which Protected Data will be Used: The exclusive purpose for which Vendor is being provided access to Protected Data is to provide Participating Educational Agencies with the functionality of the Product(s) listed above. Vendor agrees that it will not use the Protected Data for any other purposes not explicitly authorized in the MLSA. Protected Data received by Vendor, or any of Vendor's subcontractors, assignees, or other authorized agents, will not be sold, or released or used for any commercial or marketing purposes.

Oversight of Subcontractors: In the event that Vendor engages subcontractors, assignees, or other authorized agents to perform one or more of its obligations under the MLSA (including any hosting service provider), it will require those to whom it discloses Protected Data to execute legally binding agreements acknowledging the obligation under Section 2-d of the New York State Education Law to comply with the same data security and privacy standards required of Vendor under the MLSA and applicable state and federal law. Vendor will ensure that such subcontractors, assignees, or other authorized agents abide by the provisions of these agreements by providing training for information security and data privacy awareness, information security acceptable use, and code of conduct upon hire and annually thereafter.

Duration of MLSA and Protected Data Upon Expiration:

- The MLSA commences on July 1, 2023 and expires on June 30, 2026.
- Upon expiration of the MLSA without renewal, or upon termination of the MLSA prior to expiration, upon written request of Participating Educational Agency the Vendor will securely delete or otherwise destroy any and all Protected Data remaining in the possession of Vendor or its assignees or subcontractors or other authorized persons or entities to whom it has disclosed Protected Data. If requested by Erie 1 BOCES and/or any Participating Educational Agency, Vendor will assist a Participating Educational Agency in exporting all Protected Data previously received back to the Participating Educational Agency for its own use, prior to deletion, in such formats as may be requested by the Participating Educational Agency.

- In the event the Master Agreement is assigned to a successor Vendor (to the extent authorized by the Master Agreement), the Vendor will cooperate with Erie 1 BOCES as necessary to transition Protected Data to the successor Vendor prior to deletion.
- Neither Vendor nor any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data will retain any Protected Data, copies, summaries or extracts of the Protected Data, or any de-identified Protected Data, on any storage medium whatsoever. Upon request, Vendor and/or its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data, as applicable, will provide Erie 1 BOCES with a certification from an appropriate officer that these requirements have been satisfied in full.

Challenging Accuracy of Protected Data: Parents or eligible students can challenge the accuracy of any Protected Data provided by a Participating Educational Agency to Vendor, by contacting the student's district of residence regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers or principals may be able to challenge the accuracy of APPR data provided to Vendor by following the appeal process in their employing school district's applicable APPR Plan.

Data Storage and Security Protections: Any Protected Data Vendor receives will be stored on systems maintained by Vendor, or by a subcontractor under the direct control of Vendor, in a secure data center facility in North America. The measures that Vendor will take to protect Protected Data include adoption of technologies, safeguards and practices that align with the NIST Cybersecurity Framework and industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.

Encryption of Protected Data: Vendor (or, if applicable, its subcontractors) will protect Protected Data in its custody from unauthorized disclosure while in motion or at rest, using a technology or methodology specified by the secretary of the U.S. Department of HHS in guidance issued under Section 13402(H)(2) of P.L. 111-5.

EXHIBIT – E
License Agreements

aimswebPlus
SSIS Social-Emotional Learning Edition on Review360
WriteToLearn

aimswebPlus
SUBSCRIPTION AND USER LICENSE AGREEMENT

This aimswebPlus Subscription and User License Agreement ("Agreement") governs access to and use of the aimsweb fee-based products and services offered by NCS Pearson, Inc. ("PEARSON"). By accessing, using, printing, displaying or registering for such services or products, you ("CUSTOMER") agree to the terms of this Agreement in which, CUSTOMER receives a limited license to access, use, print, display or register for such services or products for an initial one school year (August 1 – July 31) period.

PLEASE CAREFULLY READ THIS AGREEMENT BEFORE ACCEPTING BELOW. PROCEEDING WITH REGISTRATION, OR ACCESSING, USING, PRINTING, OR DISPLAYING THE PRODUCTS OR SERVICES INDICATES THE CUSTOMER'S ACCEPTANCE OF THE TERMS OF THIS AGREEMENT. IF CUSTOMER DOES NOT AGREE WITH THESE TERMS, CUSTOMER SHOULD DECLINE THE REGISTRATION AND CUSTOMER MAY NOT ACCESS, USE, PRINT, OR DISPLAY THE PRODUCTS OR SERVICES.

PEARSON has developed this proprietary universal screening and progress monitoring system for academics and behavior based on direct, frequent and continuous student assessment "aimswebPlus" designed to monitor student achievement and instruction. In addition, aimswebPlus establishes and maintains a database of student performance which provides access to students, parents, teachers and administrators via a web-based data management and reporting system for providing skill assessment protocols, testing materials and instructions; assessment probes for use in the classroom (collectively referred to in this Agreement as the "MATERIALS"). Some or all of the MATERIALS are copyrighted by NCS Pearson, Inc. All of the MATERIALS are proprietary. Use of the MATERIALS by any individual, organization, entity or enterprise is strictly prohibited except for a CUSTOMER entity authorized pursuant to this Agreement.

The MATERIALS, software, online software documentation, Implementation Training Manual and the *aimswebPlus* support site (collectively the "Subscription Service") and any modifications, updates, revisions, or enhancements thereof are subject to the terms of this Agreement.

1. License Grant.

PEARSON hereby grants to CUSTOMER and CUSTOMER hereby accepts from PEARSON a limited, non-exclusive, non-transferable, revocable license to access, print and use the MATERIALS for the limited purposes of universal screening and progress monitoring for academics and behavior of each LICENSED USER associated with CUSTOMER (as defined below).

"CUSTOMER" is a person, organization, school, district, or Department of Education, public entity, business entity or enterprise which: (1) has paid a license fee to or is otherwise authorized by PEARSON to access, print and use the MATERIALS on behalf of a LICENSED USER; and (2) both CUSTOMER and LICENSED USER have agreed to be bound by the terms and conditions of this License Agreement.

"LICENSED USER" means:

(a) If CUSTOMER is a corporation, or public body such as a School, or School District, Department of Education, or similar organization, a LICENSED USER may include an individual employee or agent to whom CUSTOMER has conferred the right to use the MATERIALS or to accept these license terms. Any such individual is subject to the terms and conditions of this Agreement, and must agree to be bound and has the right to bind their organization to the terms and conditions of this License Agreement.

(b) If CUSTOMER is a post-secondary academic institution, academic library or similar research institution, a LICENSED USER may also include a post secondary student and an academic researcher, provided that CUSTOMER identifies each LICENSED USER to PEARSON and PEARSON consents to each LICENSED USER.

In this Agreement, all references to CUSTOMER shall also include LICENSED USER.

Upon expiration or termination of this Agreement, the nonexclusive limited license granted herein shall automatically and immediately terminate and CUSTOMER agrees not to access, print or use the MATERIALS and, upon request of

PEARSON, to return all MATERIALS then in possession of CUSTOMER to PEARSON or destroy and certify to PEARSON the manner and date of that CUSTOMER destroyed same.

2. Authorization.

The use of the MATERIALS is strictly limited to those provided for in this Agreement. The MATERIALS may be used only for their stated and published purposes including monitoring of student performance scores, comparison of student performance scores, individually and across various cohort groups.

CUSTOMER agrees that the MATERIALS will not be:

(a) used for any "for-profit" commercial activities, unless specifically agreed in writing by PEARSON, including any use of any trademark of PEARSON;

(b) copied, duplicated, modified, translated, adapted, publicly displayed, or publicly performed without the express written consent of PEARSON;

(c) downloaded, transmitted, or re-transmitted or transferred for the purpose of evading the prohibition on copying, duplication or modification;

(d) sold, transferred, conveyed, pledged licensed, or sub-licensed;

(e) reverse engineered, decompiled, disassembled or subject to efforts to derive source code for any software and/or computer code components of the MATERIALS; or

(f) exploited for any purpose different from or contrary to the rights and interests of PEARSON or inconsistent with the stated terms and purposes of this Agreement.

Notwithstanding the foregoing, some of the MATERIALS, including any assessment protocols, which include assessment probes, testing sheets and instructions and similar information, may be duplicated for the internal distribution and administration of student performance tests, and to train employees of CUSTOMER, including each LICENSED USER, consistent with this Agreement.

3. Ownership.

CUSTOMER is granted a non-exclusive limited license to use the MATERIALS under the terms of this Agreement. All right, title, and interest in and to the MATERIALS, the Subscription Services, and all intellectual property rights in and to the MATERIALS, the Subscription Services and the website of PEARSON, and all other materials shall remain solely vested in, to and with PEARSON. PEARSON is granted permission to use any student data received from CUSTOMER for research, development or normative purposes, as long as, such data does not contain any personally identifiable information.

4. Subscription Charges

aimswebPlus subscriptions are based on per student, per school year fees. The initial fee to activate Subscription is based on estimate by CUSTOMER of unique students that will have score data entered. PEARSON will run reconciliation reports in June of each subscription year and invoice for any overages at that time. Subscription fees are non-refundable for any reason at any time.

Certain "Subscription Services" are available only from PEARSON via a dedicated service subscription to which the following applies:

(a) CUSTOMER agrees to pay, using a valid credit card, purchase order, or check which PEARSON accepts, the subscription fees set forth by PEARSON, applicable taxes, and other charges incurred on the account of CUSTOMER in order to access, print and use the Subscription Services. PEARSON reserves the right to change fees, or to institute new fees at the end of each subscription year, upon reasonable notice posted in advance on www.aimsweb.com or as otherwise provided. aimswebPlus subscription services must be renewed on an annual basis. PEARSON does not automatically renew Subscriptions. In the event CUSTOMER chooses not to renew aimswebPlus Subscriptions, PEARSON reserves the right to terminate

CUSTOMER access to the Subscription Services. No refunds or credit will be granted for any cancellation or termination for any reason at anytime.

(b) In addition to the charges set forth above, CUSTOMER is responsible for all expenses and charges associated with accessing the internet; connecting to the Subscription Service; and any service fees associated with such access and connection. CUSTOMER is also responsible for providing all equipment necessary for CUSTOMER to make such connection, including without limitation, computer and modem and/or network connection. This includes all equipment and software used to load and print files saved in .pdf format.

(c) For purposes of identification and billing, CUSTOMER agrees to provide PEARSON with accurate, current and complete information as required during registration for the Subscription Services, including, without limitation, the legal name, address, telephone number(s), e-mail address, and applicable payment data (e.g. credit card number and expiration date) for CUSTOMER and to maintain and update this information to keep it accurate, current and complete. Failure to provide and maintain accurate, current and complete information may, at the option of PEARSON, result in immediate suspension or termination of this Agreement and the Subscription Services.

5. Multi Customer Accounts

This license for each Subscription Service creates a single account. CUSTOMER may then create additional sub-accounts, and each sub-account that CUSTOMER creates shall be fully subject to this Agreement.

6. Password

As part of the registration process for Subscription Services, CUSTOMER will select a password. CUSTOMER is solely responsible for maintaining the confidentiality of the CUSTOMER password and agrees that PEARSON has no obligations with regard to the use by third parties of such password. CUSTOMER is entirely responsible for any activity occurring under the CUSTOMER account (and any sub-account) and password. CUSTOMER agrees to notify PEARSON immediately if CUSTOMER has any reason to believe that the security of CUSTOMER data or any password has been compromised.

Should CUSTOMER forget the password, PEARSON will reset it for CUSTOMER at CUSTOMER's request; however, in order to protect the privacy of CUSTOMER and the data of CUSTOMER, PEARSON may require CUSTOMER to provide specific information.

7. Privacy & Security

PEARSON has taken reasonable actions, including use of encryption and firewalls, to ensure that data and information of CUSTOMER is disclosed only to those designated by CUSTOMER, as set forth in the applicable Privacy Policy posted on the aimsweb site. However, CUSTOMER acknowledges that the Internet is an open system and PEARSON cannot and does not warrant or guarantee that third parties will not intercept same.

8. Server Availability and Scheduled Down Times

PEARSON schedules daily maintenance from 12:00 a.m. to 6:00 a.m. Central Standard Time, Monday through Sunday. In the event a mission-critical maintenance situation arises, PEARSON may be required to perform emergency maintenance at any time. During these scheduled and emergency maintenance periods, CUSTOMER may be unable to transmit and receive data. CUSTOMER agrees to accept the risk of such unavailability and to fully cooperate with PEARSON during the scheduled and emergency maintenance periods.

9. Indemnification

To the extent permitted by law, CUSTOMER hereby agrees to indemnify, defend, and hold harmless PEARSON from and against any and all claims, proceedings, damages, liability, and costs (including reasonable attorney fees) incurred by PEARSON in connection with any claim arising out of (i) any breach or alleged breach of any of CUSTOMER obligations set forth herein, (ii) any acts by CUSTOMER, or (iii) MATERIALS or information posted or transmitted by CUSTOMER in connection with the Subscription Service regardless of the type or nature of the claim. CUSTOMER shall cooperate as fully as reasonably required in the defense of any claim. PEARSON reserves the right, at its own expense, to assume the

exclusive defense and control of any matter otherwise subject to indemnification by CUSTOMER and CUSTOMER shall not in any event settle any matter without the written consent of PEARSON.

PEARSON will hold the CUSTOMER harmless and indemnify the CUSTOMER against any third party claim that the MATERIALS, in the form delivered by PEARSON to the CUSTOMER, infringes or violates any valid United States patents or copyrights of a third party existing at the time of delivery; provided that PEARSON must be given prompt, written notice of the claim and allowed, at its option, to control the defense and settlement of any such claim. PEARSON's obligations under this Section do not apply to any infringement arising out of the use of the MATERIALS in combination with systems, equipment or computer programs not supplied by PEARSON, or any unauthorized modification of MATERIALS.

10. Limitation of Liabilities and Remedies

THE MATERIALS AND THE SUBSCRIPTION SERVICES (INCLUDING ALL CONTENT, SOFTWARE AND FUNCTIONS) ARE PROVIDED "AS IS" AND "AS AVAILABLE" AND "WITH ALL FAULTS" WITHOUT WARRANTY OF ANY KIND. PEARSON MAKES NO WARRANTY OF ANY KIND WHATSOEVER, EXPRESS OR IMPLIED. ANY AND ALL WARRANTIES ARE EXPRESSLY DISCLAIMED, INCLUDING WITHOUT LIMITATION, TITLE, SECURITY, ACCURACY, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, AVAILABILITY, OR UNINTERRUPTED ACCESS. PEARSON DISCLAIMS AND CUSTOMER WAIVES ALL LIABILITY ARISING FROM THE ACCESS, USE AND PRINTING OF THE MATERIALS AND PROVISION OF THE MATERIALS AND THE SUBSCRIPTION SERVICES.

IN NO EVENT SHALL THE LIABILITY OF PEARSON TO CUSTOMER OR ANY THIRD PARTY FOR DAMAGES FOR ANY CAUSE WHATSOEVER RELATED TO OR ARISING OUT OF THIS AGREEMENT EXCEED THE AMOUNT PAID BY CUSTOMER TO PEARSON DURING THE PRECEDING TWELVE MONTHS. IN NO EVENT WILL PEARSON BE LIABLE FOR ANY LOST PROFITS, INCIDENTAL, CONSEQUENTIAL, SPECIAL OR PUNITIVE DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE ANY MATERIALS OR THE SUBSCRIPTION SERVICE EVEN IF PEARSON HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. CUSTOMER AGREES THAT ANY CLAIM ARISING FROM USE OF OR ACCESS TO THE MATERIALS PROVISION OF ANY SUBSCRIPTION SERVICES MUST BE MADE WITHIN ONE (1) YEAR OF THE FIRST DATE SUCH CLAIM FIRST ACCRUED OR SHALL BE DISMISSED AS UNTIMELY AND FOREVER BARRED.

THIS LIMITATION OF LIABILITY APPLIES TO ANY EXPENSES, DAMAGES OR INJURY CAUSED BY ANY FAILURE OF PERFORMANCE, ERROR OF OMISSION, INTERRUPTION, DELETION, DEFECT, DELAY IN OPERATION OR TRANSMISSION, COMPUTER VIRUS, COMMUNICATION LINE FAILURE, THEFT, DESTRUCTION, OR UNAUTHORIZED ACCESS TO, ALTERATION OF, OR USE OF DATA RECORDS, WHETHER FOR BREACH OF CONTRACT, STRICT LIABILITY, TORTUOUS BEHAVIOR, NEGLIGENCE, OR FOR ANY OTHER CAUSE OF ACTION.

11. Term and Termination

This Agreement has a term of one (1) school year (August 1 – July 31) and must be renewed each following school years by CUSTOMER for continued service.

Either CUSTOMER or PEARSON may cancel or terminate this Agreement upon thirty (30) days written notice to the other via electronic mail or conventional mail, and all fees for the then-present term of this Agreement shall immediately become fully due and payable.

PEARSON reserves the right to restrict, suspend or terminate CUSTOMER access to the Subscription Services in whole or in part without notice and without liability, with respect to any breach or threatened breach of any portion of this Agreement. If PEARSON terminates this Agreement based on a breach of any portion of this Agreement, PEARSON reserves the right to refuse to provide Subscription Services to CUSTOMER.

Subject to the PEARSON Privacy Policy, if the Agreement is terminated by PEARSON for reasons other than breach of this Agreement by CUSTOMER, any student data entered by CUSTOMER will be made available to CUSTOMER either through a third party offsite vault storage provider or directly from PEARSON for up to ninety (90) days after termination. Charges may apply.

12. Modifications to License Agreement and Subscription Services

PEARSON reserves the right to modify this Agreement, and the software or policies associated with the Subscription Services and any MATERIALS at anytime without advance notice to CUSTOMER. Any modification shall take effect immediately when same is posted to www.aimsweb.com. CUSTOMER may not assign, sell, distribute, lease, rent, sublicense, or transfer the Subscription Service or the license granted CUSTOMER herein or disclose the Subscription Service to any other person. CUSTOMER continued use of the Subscription Services following any modification shall be conclusively deemed an acceptance of all such modification(s). PEARSON reserves the right to modify, suspend or discontinue the Subscription Services or any portion thereof at any time, including the availability of any functional area of the Subscription Service. PEARSON may also impose limits on certain features and services or restrict CUSTOMER access thereto without notice or liability.

13. Student Data Escrow

CUSTOMER has the ability to export their data at any time. However, PEARSON will produce regular backups of any student data of CUSTOMER and will escrow these backups. Assuming all fees owed by CUSTOMER are current and have been paid, CUSTOMER may request that any of the student data of CUSTOMER be copied to physical data storage media and provided to CUSTOMER. Charges will apply for this service. This service (receiving data) will be available to CUSTOMER only during the term of this Agreement and for a maximum period of three (3) months following the termination or expiration of this Agreement. After the three (3) month period expires, all such data may be destroyed and not available to CUSTOMER.

14. Support

At no additional charge, each CUSTOMER may use a comprehensive online customer service and assistance service. PEARSON agrees to exert reasonable efforts to provide customer service to CUSTOMER, as well as toll-free telephone and e-mail support, but each form of support is provided "**AS IS**" and "AS AVAILABLE" basis and CUSTOMER acknowledges that use of such support is at the sole risk of CUSTOMER. The support services may be changed at anytime without notice to CUSTOMER or may be discontinued in the sole discretion of PEARSON at anytime.

15. Recommended Environment

Any modification, derivative work, translation, or adaptation to the MATERIALS or the Subscription Services by CUSTOMER shall be subject to a royalty-free, non-exclusive, irrevocable worldwide license to PEARSON in and to same. CUSTOMER agrees to promptly report to PEARSON all defects, inconsistencies, or issues arising from the MATERIALS and the Subscription Services. CUSTOMER acknowledges that additional maintenance fees and upgrade costs may accrue in the event that PEARSON provides support for and/or is requested by CUSTOMER to rectify issues related thereto.

16. Student Assessment

The use, accuracy and efficacy of the Subscription Service depend in large measure upon the accuracy and completeness of the data provided to PEARSON by CUSTOMER. CUSTOMER agrees that it will use the MATERIALS, and in particular the basic skill performance tests, protocols, reading passages, testing procedures, testing instructions and all similar documents and information in a manner consistent with this Agreement, and applicable guidelines and directions from PEARSON.

17. Software Documentation Manual

PEARSON provides a variety of documentation manuals in electronic form and PEARSON hereby agrees to permit CUSTOMER to access, use, reproduce, print and distribute each applicable Documentation Manual for the internal training, educational and assessment purposes of CUSTOMER.

18. Acceptance

This Agreement must be accepted by CUSTOMER and PEARSON. CUSTOMER may indicate acceptance of this Agreement by: (1) signing and returning to PEARSON the printed acceptance form; (2) by electronic acceptance indicating that CUSTOMER accepts the Agreement; or (3) by accessing, printing, displaying and/or use of the MATERIALS or ordering any of the packages of Subscription Services. If CUSTOMER submits a purchase order for any

products or services covered by this Agreement, CUSTOMER agrees that any pre-printed terms of such purchase order shall not apply or modify this Agreement and that this Agreement shall solely control and govern the transaction and such purchase order shall constitute acceptance of this Agreement.

The laws of the State of Minnesota shall govern this Agreement and the interpretation and issues of enforcement related thereto without regard to any conflicts of laws provisions therein. CUSTOMER agrees to the personal and subject matter jurisdiction of the court sitting in the State of Minnesota. In the event that any provision of this Agreement is found invalid or unenforceable pursuant to judicial decree, the remainder of this Agreement shall be valid and enforceable according to its terms. "*aimsweb*" and "*aimswebPlus*" design are trademarks of Pearson Education, Inc.

Training

NCS Pearson, Inc.
User License Agreement

IMPORTANT, READ CAREFULLY: Your use of the NCS Pearson, Inc. proprietary software program ("Review360") is subject to this End User License Agreement (the "EULA"), which is a legal agreement between you and NCS PEARSON, INC.. Consent to this EULA is necessary in order to use Review360. In addition to the restrictions contained in the EULA, your use of Review360 is subject to a certain Purchase Agreement between your employer and NCS PEARSON, INC.

ACKNOWLEDGMENT

You certify that you will at all times act within the scope of your employment in your use of Review360, and that you will not use Review 360 for your personal use or any other matters outside of the scope of your employment. You certify further that all information will be collected in accordance with the rules of your school district and applicable state and federal laws and regulations, including, without limitation, the Children's Online Privacy Protection Act (COPPA) and the Family Educational Rights and Privacy Act (FERPA).

USE OF REVIEW360

Use. Review360 is proprietary to NCS PEARSON, INC. and is protected by intellectual property rights. You are not entitled to copy or to a copy of Review360.

Passwords. You may access Review360 via confidential passwords. Please keep all passwords confidential and do not share them with third parties. You will be responsible for all activities that occur under such passwords regardless of whether you are the person who took such actions.

Ownership. All right, title, and interest, including all copyrights, patents, trademarks, trade secrets, work product, data, and all other proprietary and intellectual property rights in existence now or arising in the future in and to Review360, the use of Review360, and any other intellectual property of NCS PEARSON, INC. or arising from your use of Review360 shall remain in NCS PEARSON, INC. and you shall not acquire any interest therein. You agree to use Review360 in a manner that protects the proprietary rights of NCS PEARSON, INC., and you will comply with reasonable requests made by NCS PEARSON, INC. to allow NCS PEARSON, INC. to protect such rights.

Reverse Engineering. YOU MAY NOT GIVE THIRD PARTIES ACCESS TO REVIEW360, OR MODIFY, REVERSE ENGINEER, DECOMPILE, OR DISASSEMBLE REVIEW360. YOU SHALL NOT, AND SHALL NOT ALLOW ANY THIRD PARTY, TO (A) PREPARE ANY DERIVATIVE WORK OF REVIEW360, (B) SUBLICENSE, TRANSFER, ASSIGN, RENT, LEASE, OR OTHERWISE CONVEY REVIEW360, OR (C) REVERSE ENGINEER, DECOMPILE, TRANSLATE, DISASSEMBLE, OR OTHERWISE ATTEMPT TO DISCOVER THE SOURCE CODE FOR REVIEW360. YOU, AND ANY THIRD PARTY ACQUIRING ACCESS THROUGH YOU, SHALL NOT STUDY THE OPERATION OF REVIEW360 IN ORDER TO DEVELOP A COMPETING SYSTEM. UPON A BREACH OF THIS PROVISION, YOU SHALL PROMPTLY ASSIGN ANY RIGHTS IN SUCH SYSTEM TO NCS PEARSON, INC..

Conduct. You agree that you will not (a) modify, alter, enhance, delete, or reproduce any portion of Review360, or (b) act in a fraudulent, tortuous, malicious, illegal, or grossly negligent manner. You may not rent, lease, lend or make any commercial use of Review360.

TERMINATION. Without prejudice to any other rights, NCS PEARSON, INC. may terminate this EULA and your use of Review360 if you fail to comply with any of the terms and conditions of this EULA. In such event, you must immediately discontinue your access and use of Review360 and all of its component parts.

Suggestions. We welcome your comments and suggestions related to Review360, but please do not submit any ideas and suggestions that you consider to be confidential or proprietary to you. To the extent that you provide comments and suggestions to NCS PEARSON, INC., you agree that NCS PEARSON, INC. may use such information, without charge or limitations on use, for all purposes.
Updates to the Terms of Use. You acknowledge that from time to time we may modify the terms governing your use of Review360. Following an update, you may be asked to re-accept the EULA. You must make an online acceptance of the modified terms or discontinue use of Review360.

Governing Law / Severability. This EULA is governed by the laws of the state of Texas. If any provision of this EULA is held by a court of competent jurisdiction to be invalid or unenforceable, the remaining portions of this EULA shall remain in force and in effect and be construed so as to best effectuate the intention of the parties upon execution.

Accept Decline

Review360
Version 23.6.0.18376 **Release Notes**

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

Pearson

Table of Contents

Information Security Controls: Alignment w/NIST SP800-53r4 **3**

Overview **3**

Background **3**

The 18 Families of Information Security Controls **4**

AC – Access Control **4**

AT – Awareness and Training **4**

AU – Audit and Accountability **4**

CA – Security Assessment and Authorization **4**

CM – Configuration Management **5**

CP – Contingency Planning **5**

IA – Identification and Authentication **5**

IR – Incident Response **6**

MA – Maintenance **6**

MP – Media Protection **6**

PE – Physical and Environmental Protection **7**

PL – Planning **7**

PS – Personnel Security **7**

RA – Risk Assessment **7**

SA – System and Services Acquisition **8**

SC – System and Communications Protection **8**

SI – System and Information Integrity **9**

PM – Program Management **9**

Pearson

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.