**DATA AND INFORMATION SECURITY ADDENDUM**

 THIS DATA AND INFORMATION SECURITY ADDENDUM (“Addendum”)

forms part of that certain [*insert the name of the agreement*], as may be amended (“Agreement”) made by and between the Commonwealth of Pennsylvania, Public School Employees’ Retirement System (“PSERS”) and [*insert name of party with whom PSERS is contracting*], a [*insert jurisdiction of organization and type* ] (“Contractor”) and sets forth additional terms and conditions with respect to data and information security applicable to the Agreement.

RECITALS

 WHEREAS, PSERS and Contractor acknowledge that the Agreement will or may require: (1) PSERS or an entity or individual for or on behalf of PSERS to disclose certain data and information to Contractor; (2) Contractor to accept, collect and/or use that data and information; and (3) Contractor to create data and information; and

 WHEREAS, PSERS and Contractor desire to agree to protect and provide for the privacy and confidentiality of all such data and information.

 NOW THEREFORE, in consideration of the foregoing recitals, which are incorporated into this Addendum, and the mutual promises and undertakings hereinafter set forth, and the exchange of data and information pursuant to the Agreement and this Addendum, Contractor and PSERS agree as follows:

1. Definitions. As used in this Addendum:
	1. “Act” means the Breach of Personal Information Notification Act, Act of Dec. 22, 2005, P.L. 474, No. 94, 73 P.S. Section 2301, et. seq., as amended and enacted in the Commonwealth of Pennsylvania, including as amended by the Act of Nov. 3, 2022, P.L.2139, No. 151 and Act of June 28, 2024, P.L. 427, No. 33.
	2. “Applicable Standards” has the meaning specified in Section 2 of this Addendum.
	3. “Authorized Person” means a Contractor’s employee, subcontractor, and any other

individual or entity acting for Contractor who has:

1. PSERS’s authorization; and
2. a specific need for access to PSERS’s Confidential Information to perform Services for or on behalf of PSERS.
	1. “Computing Service” means one or more of the following:

(i) software that is installed on a desktop or server or is accessible via web-browser that in each case, involves creating, accessing, transmitting, maintaining, accepting, or hosting Commonwealth of Pennsylvania (“Commonwealth”) data or PSERS Data; and

(ii) any computing service managed infrastructure regardless of deployment model (public, private, or hybrid) or type, such as, but not limited to, software-as-a-service (SaaS) for web-based applications, infrastructure-as-a-service (IaaS) for Internet-based access to storage and computing power, or platform-as-a-service (PaaS) that gives developers the tools to build and host Web applications, that is procured through and hosted by or within a third-party vendor, licensor, contractor, or supplier (“Service Organization”) or its subcontractor(s) (commonly referred to as “Subservice Organizations”).

* 1. “Computing Services Review” means an established process to ensure the procurement and/or implementation of any Computing Service is aligned with PSERS's overall business and intellectual technology vision, strategy, goals, and policies. This term includes representation and review from all domains to pro-actively identify, manage, and mitigate risk, if any, with the Computing Service being considered. The foregoing process requires that the Service Organization (third-party vendor, licensor, contractor, or supplier), must complete the Computing Services Requirements (CSR) document provided by PSERS that is specific to the Computing Service being considered. Any procurement or use of a Computing Service requires an approved Computed Services use case.
	2. “CONUS” means any state in the Continental United States and Hawaii.
	3. “Documentation” means all documentation related to the Services, including, if applicable, a SOW.
	4. “ISP” has the meaning specified in Section 3(a) of this Addendum.
	5. “Industry Standards” means any of the following: (i) National Institute of Standards and Technology (NIST) 800 Series; (ii) NIST Cybersecurity Framework; and (iii) ISO 27001/2, and in each case, the successor thereto or their generally recognized equivalents.
	6. “Multi-Factor Authentication” means the use of two or more of the authentication methods listed below. Two-factor employs two of the methods. Three-factor employs all three methods. The authentication methods include:

(i) something you know (e.g. PIN, password, shared information);

(ii) something you possess (e.g. token, smart card, digital certificate); and

(iii) something you are (biometrics - e.g. fingerprint, voice, iris, face).

* 1. “PSERS’s Confidential Information” meansPSERS Data that is not Public Data, including information containing personally identifiable information (commonly referred to as "PII"), “personal information” as defined in the Act, protected health information (commonly referred to as "PHI"), and electronic protected health information (commonly referred to as "ePHI") as defined in regulations issued by the United States Department of Health and Human Services, investment portfolio information and trade secrets. Trade secrets include limited partnership agreements, side letters, private placement memoranda, and similar information.
	2. “PSERS Data” means any data or information that Contractor creates, obtains, accesses, receives from PSERS or on behalf of PSERS, hosts, or uses in the course of its performance of the Agreement.
	3. “Public Data” means any specific data or information, regardless of form or format, that PSERS has actively and intentionally disclosed, disseminated, or made available to the public.
	4. “Security Breach” has the meaning specified in Section 4 of this Addendum.
	5. “Services” means the services and other obligations described in the Agreement, and if applicable, any SOW.
	6. “SOW” means a statement of work made in relation to Services.
1. Data Security.
	1. Compliance. Contractor shall comply with and ensure that Services are provided under the Agreement in compliance with the requirements set forth in the following Subsections (i), (ii) and (iii) (individually and collectively referred to in this Addendum as the “Applicable Standards”):
2. the information technology standards and policies as described in and subject to the terms of Appendix 1, Data and Information Security Addendum Operations Document, attached to and made part of this Addendum;

(ii) any applicable laws or regulations including:

1. CJIS and CHRIA for criminal history data;
2. HIPAA for health-related data;
3. IRS Pub 1075 and SSA for federal protected data;
4. PCI-DSS for financial data; and
5. The Act; and

(iii) Industry Standards (as defined above in Section 1 of this Addendum).

* 1. Data Protection. To the extent that Contractor’s obligations under the Agreement involve creating, accessing, transmitting, maintaining, accepting, hosting, or using PSERS Data, Contractor shall preserve the confidentiality, integrity and availability of PSERS Data by implementing and maintaining administrative, technical and physical controls that conform to Applicable Standards. Contractor shall implement security controls that provide a level of security consistent with accepted information security standards, which are commensurate with the sensitivity of the PSERS Data to be protected.
	2. Data Use and Access. Contractor shall use PSERS Data only and exclusively to support the performance of Services and not for any other purpose, including the use of PSERS Data in any manner that relates to computing referred to as “artificial intelligence.” With the exception of Public Data, absent PSERS’s prior written consent or as required by law, Contractor shall not disclose to or allow access to PSERS Data by any person, other than an Authorized Person in connection with the performance of Services and PSERS’s authorized employees and agents who have a need to know to perform their services for PSERS. If such disclosure is required by law, Contractor shall notify PSERS in writing before such disclosure, unless such notification is prohibited by law.
	3. Access to PSERS’s Specific Systems, Data and Services. Contractor shall limit access to PSERS-specific systems, data, and services, and provide access only, to Authorized Persons located within CONUS.
	4. Data Hosting. Contractor shall only host, store, or backup PSERS Data in physical locations within the CONUS.
	5. Multi-Factor Authentication. For services or applications exposed to the Internet, where sensitive data or information is stored, accessed, processed, or transmitted, Contractor shall provide Multi-Factor Authentication for user authentication to the web application via workstation and mobile browsers. If a service is provided via mobile application, Contractor shall cause that application to be protected by Multi-Factor Authentication.
	6. Data Backup. If appropriate to protect the integrity and availability of PSERS Data in accordance with accepted industry practice, Contractor shall maintain (and cause any third-party hosting company that it uses to maintain) a means to backup and recover PSERS Data if PSERS Data is lost, corrupted or destroyed. Contractor shall store backups offline to prevent modification or encryption by ransomware or other malicious software. PSERS shall have the right to establish backup security for PSERS Data and to keep backup PSERS Data and PSERS Data files in its possession or control in PSERS’s sole discretion.
	7. Return of PSERS Data. Upon PSERS’s request, Contractor shall ensure that PSERS can retrieve PSERS’s Data in the event Contractor is unable to continue providing Services for any reason or as a result of the termination of the Agreement. In the event of a termination and upon PSERS’s request, Contractor shall provide PSERS Data in a mutually acceptable format.

(i) Effect of Termination on PSERS Data Retention. Upon the first to occur of the termination of the Agreement for any reason or notice of such termination having been given, the provisions of this Subsection (i) shall apply notwithstanding anything contained in the Agreement or this Addendum to the contrary. Unless otherwise directed by PSERS in writing, Contractor shall maintain PSERS Data and continue to extend the protections of the Agreement and this Addendum to such PSERS Data for a period of six (6) months at which point it shall return, and then upon PSERS’s written direction destroy, all PSERS Data received from PSERS (or created or received by Contractor on behalf of PSERS) regardless of form, and shall retain no copies of PSERS Data. Contractor shall certify in writing to PSERS that these actions have been completed within thirty (30) days after receipt of PSERS’s direction to destroy. If return or destruction of PSERS Data is not feasible, Contractor shall:

(i) promptly inform PSERS that the return or destruction, as applicable, is not feasible;

(ii) continue to extend the protections of the Agreement and this Addendum to such PSERS Data; and

(iii) limit further use of PSERS Data to those purposes that make the return or destruction of PSERS’s Data infeasible.

(j) Destruction of PSERS Data. Subject to Subsection (i) above, Contractor shall erase, destroy, and/or render unrecoverable all PSERS Data in Contractor’s possession or control that is no longer required for the performance of Services. Upon PSERS’s request, Contractor shall certify in writing that these actions have been completed within seven (7) days of PSERS’s request.

1. Contractor Security.
	1. Information Security Program. Contractor represents and agrees that Contractor has in place and will continue to maintain a formal information security program (“ISP”) with written policies and procedures consistent with Industry Standards and reasonably designed to protect the confidentiality and integrity of PSERS Data when such PSERS Data is in the possession or control of Contractor. The ISP shall include administrative, technical, and physical safeguards. The safeguards shall appropriately:
2. relate to the type of data and information concerned;

(ii) be reasonably designed to maintain the integrity, confidentiality, and availability of the data and information;

(iii) protect against anticipated threats or hazards to the security or integrity of the data and information;

(iv) protect against unauthorized access to or use of the data and information that could result in substantial harm or inconvenience to PSERS;

(v) provide for secure disposal of the data and information; and

(vi) prescribe actions to be taken in the event that a security incident occurs or is suspected to have occurred.

* 1. Contractor Personnel. Contractor agrees that it shall only use Authorized Persons who are highly qualified in performing under the Agreement and have passed a background check. Contractor shall use the background check required under the Appendix 1 for individuals described therein and for all others, a background check that is recognized under Industry Standards as appropriate to address the security concerns that apply to the specific individual and the services to be provided by the individual under the Agreement.
	2. Acceptance of Acceptable Use Policy. Contractor shall ensure that all Contractor employees and other individuals acting for Contractor, who access or could access PSERS’s network as a part of performing under the Agreement, have agreed to PSERS’s Acceptable Use Policy as found in Management Directive 205.34 Amended, as it may be amended and any successor thereto (the current version being located at: <https://www.pa.gov/content/dam/copapwp-pagov/en/oa/documents/policies/md/200/205_34.pdf>), before such access.
	3. Security Awareness Training. Contractor shall ensure that its employees, agents, contractors, subcontractors are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with Applicable Standards.
1. Documentation and Required Notification.
	1. Security Incident Handling. As part of the ISP, Contractor represents and agrees that Contractor has in place and will continue to maintain a documented security incident management process. The security incident management process shall:
2. provide for the timely detection of security incidents and responses thereto; and

(ii) require the recordation of the applicable facts of each security incident and responses thereto, including the application or non-application of the security incident management process, escalation procedures, and the responsibilities of each affected party.

* 1. Notice to PSERS and Response of Security Breach.
1. Contractor shall notify by telephone PSERS’s Chief Information Security Officer at (717) 720-4699 and Deputy Executive Director for Administration at (717) 720-4825 and by e-mail PSERS at RA-PSISO@pa.gov:

(A) as soon as reasonably practicable and in any event within twenty-four (24) hours of first having knowledge or reasonable suspicion of:

(1) an unauthorized access, use, release, disclosure, or acquisition of PSERS Data;

(2) a loss, destruction, alteration, theft or corruption of PSERS Data;

(3) any event that creates a substantial risk to the confidentiality, integrity or availability of PSERS Data;

(4) a breach of any of Contractor’s security obligations under this Addendum;

(5) the occurrence of an event described in clauses (1), (2), or (3) (without reference to PSERS Data) involving data or information other than PSERS Data if Contractor has not reasonably determined that such event will not be an event described in clause (1), (2) or (3); or

(6) any other event requiring notification under applicable law, including the Act (each of the events described in clauses (1) – (5) and this clause (6)) is hereinafter referred to as a “Security Breach”), and

(B) within ten (10) days of having a suspicion that a Security Breach may have occurred unless after investigation appropriate to the suspicion during such ten (10) day period, Contractor has reasonably concluded that no Security Breach occurred.

PSERS shall provide updated contact information to Contractor within ten (10) business days of any change to the PSERS’s contact information set forth in this Subsection (i).

(ii) In the event of a Security Breach and as soon as practicable after first having knowledge of the Security Breach, Contractor shall:

* + 1. preserve forensic evidence, mitigate any potential harm, and eliminate the cause of the risk or breach within Contractor's reasonable control; and
		2. undertake a thorough forensic investigation of any compromise or improper use and provide to PSERS all information necessary to enable PSERS to fully understand the nature and extent of the compromise or improper use to the extent known.

(iii) To the extent that the Security Breach is attributable to the actions or failure to act by Contractor or Authorized Persons or breach of this Addendum by Contractor or Authorized Persons, Contractor shall at its sole expense provide timely notice to all individuals that may require notice under applicable law or regulation and an individual who would be entitled to notice under the Act, if such individual was a resident of the Commonwealth. The notice must be pre-approved by PSERS. At PSERS request, Contractor shall provide credit monitoring services to all individuals that may be impacted by the events requiring notice as described in this Section 4. Contractor agrees that it is doing business in the Commonwealth.

* 1. Security Incident Investigations. Contractor agrees to cooperate with PSERS in investigating a security incident, as declared by PSERS in PSERS’s sole discretion, and provide the names and contact information, of at least two (2) security contacts who shall respond to PSERS in a timely manner, dependent on criticality, in the event that PSERS must investigate a security incident. The current security contacts are:

Contact Names: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
Phone Numbers: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
Email Addresses: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Contractor shall provide updated contact information to PSERS within ten (10) business days of any change to the currently applicable security contact information provided to PSERS.

1. Maintenance of Safeguards.
	1. Contractor shall maintain and follow Applicable Standards with respect to any of

PSERS's Confidential Information in Contractor's possession or control and protect such information against any loss, alteration, theft or corruption.

* 1. At PSERS's request, Contractor shall provide PSERS with copies of its information security policies, processes, and procedures. Contractor shall notify PSERS within ten (10) business days of any changes to its policies, processes or procedures that relate to the security of PSERS Data in Contractor's possession or control.
1. Information Security Audit.
	1. PSERS’s Right to Review ISP and Onsite Assessment. PSERS shall have the right to review Contractor’s ISP at any time that Contractor is subject to the terms of this Addendum. During the performance of the Services, on an ongoing basis annually and immediately in the event of a Security Breach, PSERS, including its professional advisors and auditors, at its own expense, shall be entitled to perform, or to have performed, an on-site assessment of Contractor’s ISP. Contractor agrees that the assessment scope will address the services provided to PSERS, including related people, process, and technology.
	2. System and Organization Controls (SOC) Reporting. PSERS shall have the right to review Contractor’s ISP through Contractor's annual submission to PSERS of its current SOC report(s) as required to be provided under this Addendum. Upon the written request of PSERS, Contractor shall submit:
2. a SOC 1 Type II report, if hosting financial information;

(ii) a SOC 2 Type II report, if hosting, handling or processing PSERS’s Confidential Information; and

(iii) a SOC for Cybersecurity Report if any of the following conditions exist:

(A) reoccurring findings in SOC 1-Type II or SOC 2-Type II reports;

1. a cybersecurity incident or security breach has occurred;
2. cybersecurity incidents or breaches are not being detected, prevented, reported, and/or mitigated in a timely manner (as determined by PSERS);
3. cybersecurity incidents or breaches are not being properly managed by Contractor;
4. uncertainty that Contractor has an effective cybersecurity risk management program;
5. Contractor has been engaged in a merger or acquisition during the term of the Agreement; or
6. Contractor has restructured its service offerings and/or business model.

Any report required to be provided under Subsections (i), (ii) and (iii) above shall document an assessment conducted by a qualified, independent third party. The assessment scope must address the services provided to PSERS, including related people, process, and technology.

* 1. Assessment Questionnaire. Upon PSERS’s request but not more frequently than annually, Contractor agrees to complete within forty-five (45 days) of receipt of PSERS’s request an assessment questionnaire provided by PSERS regarding Contractor’s ISP, including artifacts for a subset of controls.
1. Software Development Security. In the event that Contractor conducts application software development for PSERS, Contractor shall:

(a) either make source codes available for review by PSERS or shall conduct source code scanning using a commercial security tool;

(b) cause scans to be conducted annually and at any time significant code changes are made;

(c) make scan reports available to PSERS within two (2) weeks of execution;

(d) disclose remediation timelines for high, medium and low risk security code defects; and

(e) perform scans before code is implemented in production. Contractor agrees that high risk security code defects may not be implemented in production without written approval from either PSERS’s Executive Director or a Deputy Executive Director.

1. Computing Service Clearances. Contractor shall meet the following requirements to the extent that Contractor provides a Computing Service or any change to a Computing Service pursuant to the Agreement that occurs on or after the effective date of the Agreement:
	1. Computing Service Review. Contractor shall coordinate with PSERS to complete and submit to PSERS the Computing Services Requirements (CSR) document provided by PSERS as part of the Computing Services Review. Contractor agrees that Computing Service Review and approval is required prior to implementing a Computing Service.
	2. Computing Services Requirements and Assessment Questionnaire. Contractor represents, warrants and agrees to and with PSERS that all verbal and written information that Contractor provides or is provided on behalf of the Contractor to PSERS as part of or related to each of the following, whether before or on or after the effective date of the Agreement, does not contain any untrue statement of material fact or omit to state a material fact necessary to make the statement not misleading:

(i) the Computing Services Requirements (CSR); and

1. the assessment questionnaire referred to in Section 6(c) of this Addendum.

Contractor agrees to immediately inform PSERS if any such information is untrue, ceases to be true or omits to state a material fact necessary to make the information not misleading.

1. Additional On-Going Contractor Obligations.
	1. Monitoring and Audit Logging. Contractor shall ensure system monitoring and security audit logging is enabled and accessible to PSERS’s Chief Information Security Officer or designee. Contractor shall:
2. provide monitoring (in addition, PSERS recommends verbose logging);

(ii) provide software with ability to correlate events and create security alerts; and

(iii) maintain reports that are easily accessible and in a readable format online for a minimum of 90 days and archived for a minimum of one (1) year.

* 1. Data Segmentation / Boundary Protection. Upon request, Contractor shall provide PSERS with a network/architecture diagram showing what technical controls are performing the network segmentation. If a solution spans more than one hosting environment (such as integration to PSERS’s managed environments, or across multiple hosting providers), Contractor shall provide PSERS with details on what solution components and data are deployed in which environment and:
1. include border gateway, perimeter and/or network firewall, web application firewall, VPN tunnels, security zone access as applicable to the solution;

(ii) describe data encryption methods at rest and in transit across environments; and

(iii) include the direction of connectivity (specify whether initiated inbound, outbound, or both) and specifications for API calls, protocols, etc. Contractor shall describe how data segregation (physically or logically) of PSERS Data from non-PSERS data is guaranteed and maintain the diagram as long as Contractor is subject to the terms of this Addendum and provide updates if changes occur.

* 1. Exploit and Malware Protection. Contractor shall provide security controls required to identify attacks, identify changes to files, protect against malware, protect user web services, data loss prevention (DLP) and to perform forensic analysis. Contractor shall provide:
1. file Integrity Monitoring Controls;

(ii) Anti-Malware and Antivirus Controls;

(iii) Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) Controls;

(iv) Data Loss Prevention (DLP) Controls;

(v) Forensic Controls; and

(vi) Advanced Persistent Threat (APT) Controls.

(d) Encryption. Contractor shall enable industry standard strong encryption for all records involved with Software as a Service (SaaS). Contractor shall provide technical controls with strong encryption to protect Data in Transit and Data at Rest.

(e) Identity & Access Management. Contractor shall provide technical controls for authenticating users, provisioning and deprovisioning users, identity interaction and nonrepudiation needs for administrators, internet users and internal users. Multi-Factor Authentication (MFA) shall be implemented by the Contractor for users requiring direct access to any PSERS’s application from outside the Commonwealth network. Where possible, the Commonwealth MFA solution shall be utilized.

(f) Vulnerability Assessment. Contractor shall ensure all applications are securely coded, vetted and scanned. Contractor shall:

1. conduct a third-party independent vulnerability assessment annually or sooner if due to compliance regulations or other requirements, or upon a major change to the solution;

(ii) provide vulnerability assessment results to PSERS on an annual basis during the period the Contractor is subject to the terms of this Addendum;

(iii) identify and validate vulnerabilities required for remediation; and

(iv) ensure patching is up to date.

(g) Data Protection / Recovery. Upon PSERS’s request, Contractor shall provide a business continuity plan that addresses:

1. Data/Database Recovery;

1. Application Recovery;
2. Operating System Recovery; and
3. Infrastructure Recovery.

In connection therewith, Contractor shall describe:

1. its capability to do a complete restoration in the event of a disaster;
2. what tests are performed as part of its disaster recovery plan; and
3. its capability to provide services during a pandemic event.

(h) Inventory. Contractor shall ensure a complete, accurate and up-to-date inventory of PSERS’s deployed resources within the infrastructure supporting PSERS’s deployed resources is maintained and upon request, made available for review by PSERS..

1. Compliance with Applicable Federal, State and Local Laws. Contractor shall comply with all applicable federal, state, and local laws concerning data protection, data security, data privacy and data breach notification laws, including but not limited to, the Act in the performance of the Agreement, including this Addendum.
2. Enforcing Compliance. Contractor shall enforce and be responsible for compliance by its employees, agents, and subcontractors with the provisions of this Addendum and all other confidentiality obligations owed to PSERS. Contractor shall be deemed in control of, be responsible and liable for the acts and omissions of its agents and subcontractors, including all Authorized Persons.
3. Accommodation of Additional Protections. Contractor agrees to comply with such additional protections as PSERS shall reasonably request.
4. Termination. If PSERS determines that the Contractor has breached any provision of this Addendum, such breach shall constitute a material breach of the Agreement and shall provide grounds for immediate termination of the Agreement by PSERS pursuant to the Agreement.
5. Indemnification.

(a) Contractor agrees to indemnify and hold harmless PSERS, its trustees, officers and employees (individually and collectively “Indemnified Party”) from and against all losses, damages, costs, expenses and other harm which any of the Indemnified Parties may incur, be responsible for or pay, as a result of, or arising directly or indirectly out of or in connection with, (i) Contractor's failure to meet any of its obligations under this Addendum and (ii) Security Breaches.

1. Contractor agrees to indemnify, hold harmless and defend Indemnified Party from and against all third party claims, demands, losses, awards, judgments, actions and proceedings (including Indemnified Party’s costs and expenses incidental thereto (including costs of defense and attorneys’ fees)) which any Indemnified Party may incur, be responsible for or pay, arising out of or in any way connected with Contractor’s performance or failure to perform under this Addendum.

PSERS shall provide Contractor with prompt notice of any claim or suit of which it learns to which the obligation to defend under this Section 14(b) applies.

1. Pursuant to the Commonwealth Attorneys Act, Act of October 15, 1980, P.L. 950, No. 164, as amended, 71 P.S. § 732-101—732-506, the Office of Attorney General (OAG) has the sole authority to represent PSERS in actions brought against PSERS. The OAG, however, in its sole discretion and under the terms it deems appropriate, may delegate its right of defense. If OAG delegates the defense to Contractor, PSERS will cooperate with all reasonable requests of Contractor made in the defense of such suits.
2. Neither Contractor nor PSERS may enter into a settlement of any claim or suit to which this Section 14(b) of this Addendum applies without the other party's written consent, which will not be unreasonably withheld. PSERS may, in its sole discretion, allow Contractor to control the defense and any related settlement negotiations.

(c) Contractor agrees that any limitations on Contractor's liability, regardless of conflicting language elsewhere in the Agreement, shall not limit the Contractor’s liability under this Section 14.

1. Changes to Information Technologies Standards and Policies. During the period that Contractor is subject to the terms of this Addendum, Contractor acknowledges and agrees that:

(a) the information technology standards and policies referenced in this Addendum, including Appendix 1, may change, be replaced or supplemented; or

(b) PSERS may need to change, replace or supplement such information technology standards and policies to address:

(i) changes in requirements applicable to PSERS; or

(ii) changes in information systems, including, hardware, software, networks, cloud services and data that is collected, stored, processed and distributed.

Upon written notice from PSERS that sets forth the changes and implementation timelines required by PSERS, Contractor agrees to comply with such changes and implementation timelines.

1. Survival; Order of Precedence. Notwithstanding anything contained this Addendum or the Agreement to the contrary, Contractor agrees that the obligations imposed on Contractor under this Addendum shall:
2. apply during the term of the Agreement;
3. survive the termination of the Agreement for such other period of time as may be necessary to effectuate the intended purpose of protecting PSERS Data, systems, and services; and
4. in the event of any conflict with any term of the Agreement, the terms of this Addendum shall govern and take precedence.
5. Assignment. Contractor may not assign any of its rights, duties or obligations under this Addendum without PSERS’s prior written consent.
6. Intellectual Property Infringement Indemnification.
	1. Contractor agrees to indemnify, hold harmless and defend PSERS, its trustees, officers and employees (individually and collectively “Indemnified Party”) from any and all claims brought against Indemnified Party alleging that the Services and/or Documentation or PSERS's use of the Services and/or Documentation constitutes a misappropriation or infringement of intellectual property (“IP”) of any third party. Contractor hereby agrees to be responsible for all losses, liabilities, damages, judgments, costs or expenses, including reasonable attorneys' fees awarded or resulting from any claim. PSERS shall provide Contractor with prompt notice of any claim or suit of which it learns to which the obligation to defend under this Section 18 applies.
	2. Pursuant to the Commonwealth Attorneys Act, Act of October 15, 1980, P.L. 950, No. 164, as amended, 71 P.S. § 732-101—732-506, the Office of Attorney General (OAG) has the sole authority to represent PSERS in actions brought against PSERS. The OAG, however, in its sole discretion and under the terms it deems appropriate, may delegate its right of defense. If OAG delegates the defense to Contractor, PSERS will cooperate with all reasonable requests of Contractor made in the defense of such suits.
	3. Neither Contractor nor PSERS may enter into a settlement of any claim or suit to which this Section 18(b) of this Addendum applies without the other party's written consent, which will not be unreasonably withheld. PSERS may, in its sole discretion, allow Contractor to control the defense and any related settlement negotiations.
	4. Contractor hereby agrees that any limitations on Contractor's liability, regardless of conflicting language elsewhere in the Agreement, shall not limit the Contractor’s liability under this Section 18.
7. Contractor Liability Insurance. Contractor shall procure, and maintain for the duration of the Agreement and for such other period of time that Contractor is obligated under this Addendum to protect PSERS Data, system, and services, insurance against claims and damages which may arise from or in connection with the performance of its work to include IP infringement and privacy or data breaches coverage. Coverage shall have limits of no less than $5,000,000.00 per occurrence and $10,000,000.00 aggregate. Prior to commencing Services under the Agreement, and annually thereafter, Contractor shall provide PSERS with a copy of each current certificate of insurance required by this Section 19. The certificates shall name PSERS as an additional insured and shall contain a provision that coverages afforded under the policies will not be canceled or changed in such a way to cause the coverage to fail to comply with the requirements of this Section 19 until at least 15 days’ prior written notice has been given to PSERS. Such cancellation or change shall not relieve Contractor of its continuing obligation to maintain insurance coverage in accordance with this Section 19.
8. Notices. Except as provided in [Section 4(b)(i) of this Addendum] above, as to matters requiring notice covered by this Addendum, PSERS and Contractor agree that the notice provisions in the Agreement shall apply.
9. Applicable Law and Forum. This Addendum is governed by and shall be interpreted and enforced in accordance with the laws of the Commonwealth of Pennsylvania (without regard to any conflict of laws provisions) and the decisions of Pennsylvania courts. Contractor consents to the jurisdiction of any court of the Commonwealth of Pennsylvania and any federal courts in Pennsylvania, waiving any claim or defense that such forum is not convenient or proper. Contractor acknowledges that any such court will have in personam jurisdiction over it and consents to service of process in any manner authorized by Pennsylvania law.
10. No Waiver. No waiver of any provision hereof or of any right or remedy hereunder shall be effective unless in writing and signed by the party against whom such waiver is sought to be enforced. A waiver is effective only in the specific instance and for the specific purpose for which it is given and shall not be deemed a waiver of any subsequent breach or default. No delay in exercising, failure to exercise, course of dealing with respect to, or partial exercise of any right or remedy shall constitute a waiver of any other right or remedy, or future exercise thereof.
11. Severability. If any term, covenant, or condition of this Addendum or the application thereof to any person or circumstance shall, to any extent, be invalid or unenforceable, the remainder of this Addendum, or the application of such term, covenant, or condition to persons or circumstances other than to those to which is held invalid or unenforceable, shall not be affected thereby, and each term, covenant, or condition of this Addendum shall be valid and be enforced to the fullest extent permitted by law.
12. Miscellaneous. The section headings contained in this Addendum are for convenience of reference purposes only and shall not affect the meaning or interpretation of this Addendum. Wherever from the context it appears appropriate, each term stated in either the singular or the plural shall include the singular and the plural. Usage of the term “including” in this Addendum shall be deemed to be followed by the phrase “without limitation” and shall be regarded as a reference to nonexclusive and non-characterizing illustrations. Except to the extent that PSERS has agreed otherwise in writing, PSERS and Contractor hereby acknowledge and agree that PSERS has all right, title and interest in and to PSERS Data.
13. Entire Agreement. The Agreement, including any exhibits and/or schedules attached to this Agreement and this Addendum, contain the entire understanding of the parties with respect to the subject matter of the Agreement and supersedes all prior agreements, oral or written, and all other communications between the parties relating to such subject matter.

Appendix 1

**DATA AND INFORMATION SECURITY ADDENDUM OPERATIONS DOCUMENT**

**1. Purpose**

This Data and Information Security Addendum Operations Document (Appendix 1) provides the information technology standards and policies which the [*Placeholder for short-name of vendor – standard usage is Contractor*], as defined in the Data and Information Security Addendum (Addendum) to which this Appendix 1 is incorporated, and each other entity or individual that is obligated to comply (each such entity and individual, together with the Contractor, individually and collectively referred to herein as “Contracted Resources”) shall comply for purposes of Section 2 (a)(i) of the Addendum.

**2. Requirements**

Contracted Resources shall comply with and adhere to the following requirements, as may be changed, replaced or supplemented pursuant to the terms of the Addendum (“Requirements”) in the performance of the Agreement to which the Addendum forms a part. The Commonwealth of Pennsylvania (“COPA”) Chief Information Security Officer (“CISO”) and the Public School Employees’ Retirement System (“PSERS”) CISO have discretion to review and monitor performance of compliance with the Requirements.

|  | **Requirements** |
| --- | --- |
| **Information Security**  | * Ensure the location(s) of server and data centers as well as the location of the workforce accessing them are within the United States of America.
* Ensure Information Technology (IT) environments and systems that contain COPA or PSERS data comply with all the Requirements.
 |
| **Host Security** | * Promptly investigate any suspected security incidents. Implement procedures for responding to and reporting incidents or breaches.
 |
| **Software Suite Standards** | * Utilize industry standard software for Endpoint Detection Response (EDR) on all servers, desktops, and laptops that are utilized to access or host COPA or PSERS data.
* Install and maintain appropriate EDR monitoring and management agents on all servers, desktops, and laptops that are utilized to access or host COPA or PSERS data.
* Ensure systems which access or host COPA or PSERS data are being actively monitored and run weekly reports to ensure compliance EDR and anti-virus standards.
* Implement procedures to mitigate overall and specific risks of breach or misuse of COPA or PSERS IT resources and their associated damages and costs. This includes patching, internal and external scanning, and monitoring.
* Utilize industry standard anti-virus, anti-malware, host intrusion prevention, incident response procedures, monitoring, reporting, network, and application firewalls for real-time scanning, detection, removal, and blocking of potentially malicious content.
* Ensure the names, work and mobile phone numbers, and work e-mail addresses for a primary and backup contact are provided to the PSERS CISO at ra-psiso@pa.gov.
 |
| **Security Auditing and Monitor** | * Implement services for internet access monitoring, content filtering, SSL decryption and inspection.
 |
| **Web Application Firewall** | * Implement a Web Application Firewall (WAF). The WAF shall be used to protect data. In addition, the WAF shall:
	1. Minimize the threat window for each exposure by blocking access to the vulnerability until the vulnerability can be fixed in the source code;
	2. Meet HIPAA and privacy compliance requirements;
	3. Monitor end-user’s transactions with a web application; and
	4. Provide an additional layer of web application hardening Open

 Web Application Security Project (OWASP) protection. |
| **Application Certification and Accreditation** | * Scan all application code for vulnerabilities using an industry standard static and dynamic code scanning tool.
* Ensure internet facing and web facing applications applicable to this category of Requirement go through the COPA Application Certification and Accreditation (CA2) process before being deployed in production.
* Provide attestation of ongoing application code and vulnerability scanning.
* Ensure secure coding practices are built within applications according to and in alignment with the Software Development Lifecyle (SDLC) process, refer to [NIST Special Publication 800-160v1r1, Engineering Trustworthy Secure Systems](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1r1.pdf)).
* Ensure applicable applications go through the CA2 reaccreditation process every 3 years.

  |
| **Minimum Standards for IDs, Passwords, Sessions, and Multi-Factor Authentication**  | * Password policies shall be utilized, including but not limited to the requirement for complex passwords and multi-factor authentication (MFA).
* Implement multi-factor authentication (MFA) for Contracted Resources requiring direct access to a system from outside the COPA and PSERS network.
* Implement MFA for any systems containing classified or confidential data.
 |
| **Minimum Contractor Background Checks** | * Conduct background checks for each Contracted Resource and any subcontracted resources who will have access to COPA data or PSERS data or COPA or PSERS owned or leased facilities, either through onsite or remote access.
* Background checks shall be conducted via the COPA requests for criminal record check processes (see [Request a Criminal History Background Check](https://www.psp.pa.gov/Pages/Criminal-History-Background-Check.aspx)) for in-state Contracted Resources or subcontracted resources or via a criminal background check through the appropriate state agency, (see [appropriate state agency](https://www.pa.gov/content/dam/copapwp-pagov/en/dhs/documents/keepkidssafe/about/documents/c_297036.pdf)) for out of state Contracted Resources or subcontracted services.
* The background check shall be conducted prior to initial access by the Contracted Resource or subcontracted resources, and annually thereafter.
* Ensure a fingerprint database search is conducted for Contracted Resources or subcontracted resources having access to Criminal Justice Information (CJI), Federal Tax Information (FTI), Criminal History Record Information (CHRI), and PA Commonwealth Law Enforcement Assistance Network (CLEAN) by either on site or remote computer access.
* Be responsible for the payment of all fees associated with background checks for Contracted Resources or subcontracted resources.
 |
| **Virtual Private Network Standards** | * Require Virtual Private Network (VPN) access to its networks and/or connected systems.
* Utilize a VPN connection for any access to the COPA and PSERS network from an external source.
 |
| **Data Cleansing** | * Implement process(es) for the cleansing of data from electronic media when the data retention requirements have expired, the data is no longer needed, or the data is scheduled for disposal as determined by PSERS.
* Degauss, wipe or destroy decommissioned electronic media in

by following best practices outlined in [NIST Special Publication 800-88 Revision 1, Guidelines for Media Sanitization](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf)). |
| **Information Security Officer Contact for PSERS** | * Provide contact information for an Information Security Officer (ISO) and backup ISO who are responsible for all security matters related to PSERS.
 |
| **Procedures for Protecting COPA and PSERS Electronic Data** | * Utilize a web application firewall (WAF) to protect data.
* Encrypt classified and confidential data at rest using encryption standards in alignment with, but not limited to, the [National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program](https://csrc.nist.gov/projects/cryptographic-module-validation-program).
	+ For Criminal Justice Information, encryption must also meet [Criminal Justice Information Services Security (CJIS) Policy](https://www.fbi.gov/file-repository/cjis_security_policy_v5-9_20200601.pdf/view)  requirements.
	+ For systems receiving, processing, or storing Federal Tax Information (FTI), encryption must also meet IRS Publication

1075 requirements.  |
| **Security Information and Event Management**  | * Log events to include:
1. Log collection and consolidation;
2. Security event collection from multiple sources (firewalls,

routers, servers, etc.);1. Identification of security related events and incidents;
2. Automated response/alerting capability when incidents are

detected; and1. Correlation of events from multiple sources.
 |
| **Information Technology Technical Security Assessments** | * Perform assessments, audits, vulnerability scanning, and/or penetration testing consistent with industry standards.
 |
| **Cyber Security Incident Reporting**  | * Provide notice to PSERS as soon as practical upon discovery of a cyber security incident, but no later than the time period specified in the Addendum, and if applicable, the Pennsylvania Breach of Personal Information Notification Act, as amended (Act).
* Have a documented cyber security incident response process and ensure all suspected cyber security incidents are reported as required in the Addendum.
* Follow a cyber security incident response process, including, but not limited to, disconnecting a system from the network, confiscating hardware for evidence, providing information for investigative purposes.
 |
| **Proper Use and Disclosure of Personally Identifiable Information (PII)** | * Perform a data element inventory, identifying and classifying all “personally identifiable information” (PII) generated, collected, stored, used, and disclosed by PSERS or third party on PSERS’s behalf.
* Ensure access or use of information utilizing PII, or other protected data types (CJIS, FTI, HIPAA, etc.) for any purpose, is properly controlled, encrypted, and restricted to prevent unauthorized use or disclosure. For Social Security Administration (SSA) compliance, the system’s encryption methods must align with the guidelines established by NIST. SSA recommends the Advanced Encryption Standards (AES) or Triple Data Encryption Algorithm (Triple DES).
* Take appropriate measures, implement necessary technology, and establish operating procedures to ensure data privacy is maintained.
* Limit the generation, collection, storage, use, and disclosure of PII to that which is necessary for business purposes only.
* Ensure that systems that require a unique identifier do not use PII as that identifier.
* Assign a unique identification number to an individual for systems requiring it. The unique identification number cannot be the same as or cannot be traced back to users PII. Security must be applied, and care must be taken to ensure that access to the electronic system and use of these unique identification numbers are restricted in accordance with any law or other PSERS requirement.
* Ensure contracted resource and agency hosted systems do not display PII visually, whether on computer monitors, printed forms, or other system output, unless required by any law or other requirement applicable to PSERS, or business necessity.
* Report security incidents involving PII in accordance with any laws or regulations for incidents or data breaches, such as the [Act](https://www.legis.state.pa.us/cfdocs/legis/li/uconsCheck.cfm?yr=2022&sessInd=0&act=151).
 |
| **Physical Security for IT Resources** | * Implement policies and practices to ensure the protection of physical facilities and appropriate screening for facility access for any IT facility or resource hosting COPA or PSERS data.
* Ensure their personnel cooperate with COPA site requirements, which includes providing information for COPA badging and being escorted. Contracted Resources and COPA approved subcontracted resources who do not have a COPA badge, shall always display their company identification badge while on COPA premises. COPA and PSERS reserve the right to request additional photo identification from Contracted Resources and subcontracted resources.
* Document an inventory of items (such as tools and equipment) being brought onto the COPA worksite, and to submit to a physical search at COPA worksites that have this requirement for persons entering their premises such as the State Police or Department of Corrections.
	+ Ensure Contracted Resources and subcontracted resources always have a list of tools being brought onto the worksite and are prepared to present the list to a COPA employee upon arrival, as well as present the tools or equipment for inspection.
	+ Before leaving the worksite, Contracted Resources and subcontracted resources shall again present the list and the tools or equipment for inspection and may be searched by COPA staff, or a correctional or police officer.
* Restrict access to their IT facilities and resources to only authorized persons.
* Ensure their IT facilities and resources hosting or accessing COPA or PSERS data are physically protected in proportion to the data or application's criticality or functional importance.
 |
| **Encryption Standards** | * Ensure protection of COPA and PSERS data that is stored within the Contracted Resource’s systems.
* Ensure COPA and PSERS classified and confidential data are encrypted during rest and transit in alignment with industry standards, including but not limited to, [NIST Cryptographic Module Validation Program](https://csrc.nist.gov/projects/cryptographic-module-validation-program).
* Ensure use of full disk encryption for archiving and back up.
* Ensure non-Windows environments requiring full disk encryption, utilize full disk encryption that conforms to AES specifications and the [NIST Cryptographic Module Validation Program](https://csrc.nist.gov/projects/cryptographic-module-validation-program).
* Ensure use of data element encryption when COPA or PSERS classified and confidential data are stored within a database. Transparent Data Encryption (TDE) or other database specific methods can be utilized to meet this requirement.
 |
| **Data Loss Prevention (DLP)Compliance Standards** | * Implement a Data Loss Prevention (DLP) technology/solution.
 |
| **Firewall Rule Set** | * Ensure any devices with access to or hosting COPA or PSERS data are protected by a perimeter firewall system.
* An audit must be performed to identify all application service protocols to ensure specific port requirements are documented and applied to the necessary firewall(s).
 |
| **Mobile Device Security**  | * If mobile device access to COPA or PSERS resources or data is permitted, a Mobile Device Management (MDM) solution shall be implemented to manage access and protect mobile devices in the event they are lost or stolen.
 |
| **Data Center Privileged User Identification and Access Management** | * Ensure default application and/or hardware passwords are changed and managed to meet industry standard requirements, including but not limited to, MFA and complex password requirements.
 |
| **IT Service Organization Management and Requirements** | * Comply with Requirements by coordinating with respective COPA agencies to complete the Computing Services Requirements (CSR)document as part of the Use Case Review Process as and if provided and requested by the PSERS.
* Submit relevant SOC reports or other agreed upon third-party security assessment as required by the Addendum.
 |
| **Standard Patching Requirements**  | * Ensure security patches are applied in accordance with industry standards and best practices to any systems connecting to the COPA or PSERS network, or supporting COPA or PSERS systems, applications, or data, provided that compliance with this Requirement shall be deemed satisfied if monthly release patches are tested and deployed within the number of business days of the vendor release as set forth in the following schedule, as applicable:
1. For Microsoft patches:

|  |  |  |  |
| --- | --- | --- | --- |
| **Severity** | **Critical** | **Important** | **Moderate** |
| **Testing** | Immediate | 5 business days  | 10 business days |
| **Deployment** | 10 business days release | 10 business days  | 15 business days |

1. For all other vendor hardware/software patches: within 25 business days regardless of severity level.
 |