NEW YORK STATE MODEL DATA PRIVACY AGREEMENT FOR EDUCATIONAL AGENCIES

Williamson Central School District
and
Onshape, a business unit of PTC Inc.

This Data Privacy Agreement ("DPA") is by and between the Williamson Central School District ("EA"), an Educational Agency, and Onshape, a business unit of PTC Inc. ("Contractor"), collectively, the "Parties".

ARTICLE I: DEFINITIONS

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

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

8. **NIST Cybersecurity Framework**: The U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.
9. **Parent:** A parent, legal guardian or person in parental relation to the Student.
10. **Personally Identifiable Information (PII):** Means personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g, and Teacher or Principal APPR Data, as defined below.
11. **Release:** Shall have the same meaning as Disclose.
12. **School:** Any public elementary or secondary school including a charter school, universal pre-kindergarten program authorized pursuant to Education Law § 3602-e, an approved provider of preschool special education, any other publicly funded pre-kindergarten program, a school serving children in a special act school district as defined in Education Law § 4001, an approved private school for the education of students with disabilities, a State-supported school subject to the provisions of Article 85 of the Education Law, or a State-operated school subject to the provisions of Articles 87 or 88 of the Education Law.
13. **Student:** Any person attending or seeking to enroll in an Educational Agency.
14. **Student Data:** Personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g.
15. **Subcontractor:** Contractor's non-employee agents, consultants and/or subcontractors engaged in the provision of services pursuant to the Service Agreement.
16. **Teacher or Principal APPR Data**: Personally Identifiable Information from the records of an Educational Agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§ 3012-c and 3012-d.

ARTICLE II: PRIVACY AND SECURITY OF PII

1. **Compliance with Law.**

   In order for Contractor to provide certain services ("Services") to the EA pursuant to the Onshape Terms of Use located at https://www.onshape.com/en/legal/terms-of-use ("Service Agreement"); Contractor may receive PII regulated by several New York and federal laws and regulations, among them, the Family Educational Rights and Privacy Act ("FERPA") at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); New York Education Law Section 2-d; and the Commissioner of Education's

Regulations at 8 NYCRR Part 121. The Parties enter this DPA to address the requirements of New York law. Contractor agrees to maintain the confidentiality and security of PII in accordance with applicable New York, federal and local laws, rules and regulations.

2. **Authorized Use.**
   Contractor has no property or licensing rights or claims of ownership to PII, and Contractor must not use PII for any purpose other than to provide the Services set forth in the Service Agreement. Neither the Services provided nor the manner in which such Services are provided shall violate New York law.

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

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

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

6. **Contractor's Employees and Subcontractors**.

(a) Contractor shall only disclose PII to Contractor's employees and subcontractors who need to know the PII in order to provide the Services and the disclosure of PII shall be limited to the extent necessary to provide such Services. Contractor shall ensure that all such employees and subcontractors comply with the terms of this DPA.

(b) Contractor must ensure that each subcontractor performing functions pursuant to the Service Agreement where the subcontractor will receive or have access to PII is contractually bound by a written agreement that includes confidentiality and data security obligations equivalent to, consistent with, and no less protective than, those found in this DPA.

(c) Contractor shall examine the data security and privacy measures of its subcontractors prior to utilizing the subcontractor. If at any point a subcontractor fails to materially comply with the requirements of this DPA, Contractor shall: notify the EA and remove such subcontractor's access to PII; and, as applicable, retrieve all PII received or stored by such subcontractor and/or ensure that PII has been securely deleted and destroyed in accordance with this DPA. In the event there is an incident in which the subcontractor compromises PII, Contractor shall follow the Data Breach reporting requirements set forth herein.

(d) Contractor shall take full responsibility for the acts and omissions of its employees and subcontractors.

(e) Contractor must not disclose PII to any other party unless such disclosure is required by statute, court order or subpoena, and the Contractor makes a reasonable effort to notify the EA of the court order or subpoena in advance of compliance but in any case, provides notice to the EA no later than the time the PII is disclosed, unless such disclosure to the EA is expressly prohibited by the statute, court order or subpoena.

7. **Training**.

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

8. **Termination**

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

9. **Data Return and Destruction of Data**.

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

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

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

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

10. Commercial or Marketing Use Prohibition.

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

11. Encryption.

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

12. Breach.

(a) Contractor shall promptly notify the EA of any Breach of PII without unreasonable delay no later than seven (7) business days after discovery of the Breach.

Notifications required pursuant to this section must be in writing, given by personal delivery, e-mail transmission (if contact information is provided for the specific mode of delivery), or by registered or certified, and must to the extent available, include a description of the Breach which includes the date of the incident and the date of discovery; the types of PII affected and the number of records affected; a description of Contractor's investigation; and the contact information for representatives who can assist the EA. Notifications required by this section must be sent to the EA's District Superintendent or other head administrator with a copy to the Data Protection Office. Violations of the requirement to notify the EA shall be subject to a civil penalty pursuant to Education Law Section 2-d. The Breach of certain PII protected by Education Law Section 2-d may subject the Contractor to additional penalties.

(b) Notifications required under this paragraph must be provided to the EA at the following address:

[Name: Mikala Smolinski

Title: Data Protection Officer

Address: PO BOX 900

City, State, Zip: Williamson, NY, 14589

Email: msmolinski@williamsoncentral.org]

13. Cooperation with Investigations.

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

14. Notification to Individuals.

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

15. Termination.

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

ARTICLE III: PARENT AND ELIGIBLE STUDENT PROVISIONS

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

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

ARTICLE IV: MISCELLANEOUS

1. **Priority of Agreements and Precedence.**

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

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

EDUCATIONAL AGENCY	Onshape, a business unit of PTC Inc.
BY: Mikala Smolinski	By: DocuSigned by: Erin Christenson DE17C264BCC44DA...
Printed Name: Mikala Smolinski	Printed Name: Charles Dunn Erin Christenson
Title: Data Protection Officer	Title: SVP Global Data Privacy Officer Sr Corp Counsel
Date: 4/25/25	Date: 28 April 2025

PTC Addendum to New York State Model Data Privacy Agreement for Educational Agencies

The parties hereto agree to the following modifications to the DPA:

1. 1. Notwithstanding anything to the contrary in the DPA, where compliance with EA policies is required under the DPA, this shall be deemed to mean policies set forth in the DPA or otherwise provided and accepted in writing by Contractor. Contractor shall make reasonable efforts to notify EA in advance if it determines that it cannot comply with any local laws or EA policies. To the extent that Contractor is unable to comply with any local laws or EA's policies, then it shall not be deemed a material breach of contract, provided either party shall have the right to immediately terminate the Agreement upon notice to the other party. In such cases, Contractor shall provide the EA with a pro rata refund of any prepaid but unused fees.
2. Article II, Section 5: In lieu of copies of PTC's security and data privacy related policies, PTC may provide summaries of such.
3. Article II, Section 6(b) is hereby deleted and replaced as follows: Contractor must ensure that each subcontractor performing functions pursuant to the Service Agreement where the subcontractor will receive or have access to PII complies with data privacy terms consistent with those required of Contractor in this DPA.
4. In Article II, Section 6(c), the second sentence is hereby deleted and replaced as follows: If at any point Contractor discovers that a subcontractor fails to materially comply with the requirements of this DPA, Contractor shall: remove such subcontractor's access to PII; and, as applicable, retrieve all PII received or stored by such subcontractor and/or ensure that PII has been securely deleted and destroyed in accordance with this DPA. In the event there is an incident in which the subcontractor compromises PII, Contractor shall follow the Data Breach reporting requirements set forth herein.
5. Article II, Section 9(a) is deleted in its entirety and replaced with the following: Upon written request from the EA to dispose of Student Data, Contractor shall promptly delete such Data subject to Contractor's data retention and backup policies. Upon termination of this Agreement, all Student Data will be deleted from online systems 60 days after the termination of the Agreement. Student Data stored in backups are subject to Contractor's backup and data retention policy. As of the execution date of this Agreement, PTC Onshape's backup and data retention policy requires PTC Onshape to delete all backups older than 1 year. Contractor may maintain de-identified data that will no longer meet the definition of Student Data as set forth in this Agreement. Such information will be aggregate data to be used by the Contractor for research and development purposes only.
6. Article II, Section 14: Any payments or reimbursement for notices or credit monitoring to individuals impacted by a Security Breach shall only be provided by Onshape if required by Federal or New York State law. Note that at the time of this Agreement, New York State law requires EA to notify parents of a Security Breach by phone, email, or certified mail. Due to the relatively low-risk nature of the Student Data processed by Contractor, EA agrees to utilize phone or email unless the situation is such that sending certified mail is reasonably warranted.
7. In any conflict between this Addendum and the DPA, the terms of this Addendum will govern.

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

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

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

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

3. State and federal laws such as Education Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student's identifiable information.

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

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

6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to the EA at: https://forms.gle/yM7qdAibzvDJdM4KA or completing the form and mailing the form to the district's Data Protection Officer at the following address:

Data Protection Officer

PO Box 900

Williamson, NY, 14589

(ii) Complaints may also be submitted to the NYS Education Department at www.nysed.gov/data-privacy-security/report-improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to privacy@nysed.gov; or by telephone at 518-474-0937.

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

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

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

Onshape, a business unit of PTC Inc.

By:	DocuSigned by: Erin Christenson DE17C264BCC44DA...
Printed Name: Charles Dunn	Erin Christenson
Title: SVP Global Data Privacy Officer	Sr Corp Counsel
Date:	05 May 2025

EXHIBIT B

BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY -

SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE INFORMATION

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

Name of Contractor	Onshape, a business unit of PTC Inc.
Description of the purpose(s) for which Contractor will receive/access PII	The exclusive purpose for which Contractor is receiving PII from the District is to provide the District with the functionality of the products or services listed above. Contractor will not use PII for any other purposes not explicitly authorized.
Type of PII that Contractor will receive/access	Check all that apply: ☒ Student PII ☐ APPR Data
Contract Term	Contract Start Date ___4/25/25____________________ Contract End Date _____6/30/26___________________
Subcontractor Written Agreement Requirement	Contractor will not utilize subcontractors without a written contract that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Contract. (check applicable option) ☐ Contractor will not utilize subcontractors. ☒ Contractor will utilize subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, Contractor shall: • At the EA's option and written request, Securely transfer data to EA, in a format agreed to by the parties and further described in the DPA.

	• Securely delete and destroy data in accordance with PTC's data retention and backup policy.
Challenges to Data Accuracy	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. If a correction to data is deemed necessary, the EA will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA's written request.
Secure Storage and Data Security	Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply) ☒ Using a cloud or infrastructure owned and hosted by a third party. ☐ Using Contractor owned and hosted solution ☐ Other: Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data: Contractor will conduct periodic risk assessments and remediate any identified security vulnerabilities in a timely manner. All data in the Vendor/Third Party Contractor's possession will be securely stored. Vendor/Third Party Contractor represents that security protections, including encryption where applicable, will be in place to ensure that the data is protected. The measures that Contractor takes to protect Confidential Data will align with the NIST Cybersecurity Framework.
Encryption	Data will be encrypted while in motion and at rest.

Onshape, a business unit of PTC Inc.
By: DocuSigned by: Erin Christenson DE17C264BCC44DA...
Printed Name: Charles Dunn Erin Christenson
Title: SVP Global Data Privacy Officer Sr Corp Counsel
Date: 05 May 2025

EXHIBIT C - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

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

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	PTC/Onshape is a global company. We adhere to the rigorous standards of state, federal and applicable EU laws. Onshape's security team is comprised of: offensive (red team) engineers, defensive (blue team) engineers, and compliance experts. Onshape works with PTC's Chief Data Privacy Officer to follow all applicable laws.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	1. TLSv1.2 encryption of all information in motion 2. AES-256 encryption of all data at rest 3. A SOC 2, Type II report describing the correct design and operational effectiveness of internal controls related to the security, availability, and confidentiality of the Onshape service.
3	Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.	As part of its Compliance program PTC/Onshape requires that all employees and contractors to be trained on data protection security and confidentiality standards and regulations on hiring as part of the onboarding process, and annually thereafter.
4	Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.	All PTC employees and sub-contractors are legally bound to preserve the confidentiality of any personal information that they have access to in the course of their employment/ engagement with PTC. PTC/Onshape trains its employees who have access to personal information on maintaining confidentiality and data security in compliance with applicable state and federal laws. As part of its selection and onboarding process for vendors/subcontractors, PTC/Onshape reviews their technical and organizational measures security and privacy measures, performs appropriate data protection impact assessments, where necessary, and enters into data protection addendum agreements with those who will have access to personal information.

5	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the EA.	PTC's technical and organizational data security measures comply with industry standards and PTC will follow its data incident response plan to mitigate the impact of any data incident on any affected school or individual. PTC's data incident response policy requires those affected by an incident to be notified, via e-mail, without undue delay of PTC becoming aware of the incident.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Upon request of the EA, PII will be returned via text files and student content will be returned via CAD format.
7	Describe your secure destruction practices and how certification will be provided to the EA.	PII will remain in Onshape backups subject to our retention and deletion policies here: https://www.onshape.com/en/privacy-center/privacy-policy
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	Contractor has (a) designated an employee to coordinate its information security program, (b) identified reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of School District's Information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assessed the sufficiency of any safeguards in place to control these risks, and (c) designed and implemented information safeguards to control the risks identified through the risk assessment, and regularly tests or otherwise monitors the effectiveness of safeguards' key controls, systems and procedures. Contractor conducts periodic risk assessments and remediates any identified security vulnerabilities in a timely manner. Contractor also has an incident response plan, which includes prompt notification to the School District in the event of a security or privacy incident, as well as best practices for responding to a breach of PII.
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below.	PLEASE USE TEMPLATE BELOW.

EXHIBIT C.1 – NIST CSF TABLE

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

Function	Category	Contractor Response
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	Internal tooling maintains an inventory of all systems, including software, and is constantly monitored.
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	Cybersecurity is a risk area with oversight at the highest levels of the organization, including the Executive Level and Board. The cybersecurity program is constantly under review as we are always trying to improve and mature. PTC management is responsible for the secure operation of their information technology assets and must ensure that all reasonable actions are taken to guarantee this security. Each manager has the general responsibility for security within their areas of control. The IT Shared Services Organization is responsible for establishing basic cybersecurity controls for all desktop, laptops, and other general-purpose computers within PTC.
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	To ensure a strong governance program, PTC maintains an Enterprise Cybersecurity Policy Management program (ESPM). This cross functional team provides both management and users with a detailed understanding of the goals, approach and implemented controls for securing PTC Data and PTC Systems. This team ensures the governance is in place to protect sensitive and regulated information, including risk assessment, risk treatment, selection and implementation of security controls, ongoing evaluation, and maintenance. PTC Security policies are subject to continuous, but at least annual, review and adjustment as needed to adapt to a changing threat landscape, as part of our Enterprise Policy Management program. This program is managed through a cross functional policy review workgroup with representation from Legal, Privacy, Cybersecurity, Product Security, IT Security, Cloud Security and Compliance.

Function	Category	Contractor Response
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	PTC has established an internal Risk Management Department under Corporate Compliance that undertakes ongoing maturity assessments, reporting to the Board of Directors. We periodically engage a third-party security consulting firm to conduct an Enterprise Security Maturity Assessment. Our Cloud, IT and Product security teams have had independent focused third-party audits, based upon certification requirements or potential risk areas. Finally, Internal Audit is an independent assurance and advisory function with a direct reporting relationship to the PTC Board of Directors.
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	Please see above response.
	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	The Vendor Risk Management (VRM) program has been established to support PTC in meeting its cybersecurity, privacy, regulatory and compliance obligations and managing risk associated with Third-Party Vendors who have access to PTC IT Systems and Data. VRM is led by a dedicated VRM Program Manager reporting to the Chief Compliance Officer. Prior to outsourcing or allowing third-party access to PTC or customer Systems, IP, or data; risks associated with such activity are clearly identified and documented. The process of selecting a third-party vendor includes due diligence of the vendor service or product in question in the form of a risk assessment based on publicly available information and the vendor's response to PTC's mandatory Cybersecurity & Privacy questionnaire and review of proposed terms and conditions to ensure that PTC is not exposed to unacceptable risk.
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	Onshape uses role-based access for employees who get access to customer data. Such access is heavily monitored and only required roles/privileges are provided, as necessary. Operations personnel are allowed remote access with specific regulations from outside through the use of the VPN client. Remote access is provisioned for employees through a standard ticketing mechanism.
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness	All Onshape employees are trained in basic security and privacy hygiene during onboarding. Acceptance of PTC and Onshape

Function	Category	Contractor Response
	education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	policies are required as part of the hiring process. Acceptance records are kept in HR. The IT Security Policy statements below are part of PTC's security training program: • Statement of Management's commitment to IT Security throughout PTC • Requirement to become familiar with and comply with PTC's IT Security Policies • Statement that personal accountability for one's own actions and inactions, and general responsibilities towards securing or protecting information belonging to PTC, its customers, and third parties will be enforced • Contact points and resources for additional information and advice on IT Security matters • Methods commonly used in intrusions that can be blocked through individual action. • IT Security shall make updates to the training based on changes that occur in PTC's organizational structure, procedures, or technology that may impact IT Security requirements. If IT Security identifies such a need during the annual enterprise risk assessment or after a security incident, IT Security shall supplement training with emails, posters, or activities.
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	Onshape's Security Policy covers the following topics: • Explicitly defines the authorization boundary for the system • Describes the operational context of the information system in terms of mission and business processes. • Provides the security categorization of the information system including supporting rationale • Describe the operational environment for the information system and relationships with or connections to other information systems. • Provides an overview of the security requirements for the system • Describes the security controls that are in place at a high level • Get reviewed and approved by the authorizing official or designated representative prior to plan implementation

Function	Category	Contractor Response
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	Please see above response.
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	Onshape has not had scheduled maintenance since 2015. We engineer all changes to the production environment in real time without impacting the service. Maintenance is only done by authorized operations team members. Our service is highly available and can self-heal around outages. All changes are ticketed and reviewed. Changes are done through "Infrastructure as Code" processes and are tracked in a source code control system. Where manual changes are required, "Over the Shoulder" reviews are performed.
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	Onshape uses a modern network architecture with Virtual Private Clouds (VPCs), Security Groups (SGs) and Network Access Control Lists (NACLs) that provide fine-grained control between all instances, not just tiers. This is made possible by software-defined networking that allows us to specify only the ports and protocols that are allowed to pass between different service types. In the Onshape architecture, we define approximately 50 different “roles” (service types) that each have their own security groups. All instances are deployed via automation from Application Machine Images (AMIs) that are built three times a week by the Onshape team. These AMIs only have required services installed. Instances running these AMIs are scanned monthly with a Nexpose scanner to identify any vulnerabilities. Vulnerabilities are ticketed and remediated as part of our development process.
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood.	Onshape uses an Intrusion Detection System (IDS) with real-time alerting. The File Integrity Monitoring (FIM) alerts are monitored by a Security Operations Center (SOC) at the FIM and communicated to the Operations team. Several other tools are used as an IPS. Source IP blocking, account lockout, rate limiting and other techniques are used as countermeasures. FIM agents act as host-based intrusion detection system (HIDS) and will alert on any file changes post-installation and monitor for any unauthorized access or remote code exploitation. The FIM service is integrated with AWS accounts as well to monitor the

Function	Category	Contractor Response
		cloud control plane. FIM agents on the instances perform analysis on network traffic that leaves/enters the instances. In addition, Onshape, utilizes AWS Shield, which also performs traffic analysis to detect malicious activities within the environment, as well as on the instances. Onshape also scans all uploads for malware. Onshape also uses industry standard tools to scan our Production environment on a regular basis. Any vulnerabilities detected during the scanning process are risk rated and are handled as per PTC's Vulnerability Handling Policy. Vulnerability scans are strictly company confidential and cannot be shared externally. However, a summarized annual pen test report can be shared under strict NDA.
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	Multiple log events, metrics, intrusion detection, and network monitoring are all used as part of a continuous monitoring system in Onshape. SIEM tools are deployed within the environment for log aggregation and correlation and would notify the Ops Team when deemed necessary. Onshape has also partnered with a third party for their Security Operations Center (SOC) services. Their SOC monitors the Onshape environment @ AWS 24x7.
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	Please see response for DE.AE above.
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	PTC has a formal Incident Response Policy and Plan in place. The Onshape Security Incident Response Plan (SIRP) mandates the recording of all security incidents including data privacy violations. In addition, PTC Compliance, Legal and Corporate Communication teams are assembled as needed for incident response. Every incident response is followed up with a post-mortem/debrief.
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	PTC follows proper policy, procedure, contractual requirements, and regulatory requirements in any event regarding security breach, litigation, or regulatory enforcement actions that pertain to privacy or data security/protection. Incident handling is done by individual organizations with security responsibility and monitored/guided by applicable corporate functions. PTC's Incident Policy and Plan requires PTC to notify the affected customer without undue delay of an actual breach

Function	Category	Contractor Response
		that affects the customer's data, per negotiated contract terms.
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	Every incident response is followed up with a post-mortem/debrief.
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	Please refer to the response for RS.CO above. The team regularly reviews new threats, ticket, triages new risks and mitigate risks based on severity.
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	Yes – Please refer to the response for RS.AN above.
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	Onshape has developed and maintains a detailed contingency plan that address all of the following: • Identifies the essential missions and business functions • Provides recovery objectives, restoration priorities, and metrics ○ RPO - 8 hours. RTO -24 hours • Addresses contingency roles, responsibilities, and assigned individuals with contact information • Addresses maintaining essential missions and business functions despite a disruption • Addresses full restoration without deterioration of originally implemented security safeguards • Distributed to key personnel • Coordinated with incident handling procedures • Reviewed and updated to address changes • Protected from unauthorized disclose or modification **Plan Testing** Tabletop Disaster Recovery/Business Continuity plans are tested annually. Restore from backup to fully functioning environment is done every 3 weeks. **Disaster Recovery** Recovery starts with virtual network infrastructure (Virtual Private Clouds, security groups, Network Access Control lists)and is provisioned by automation. Next, infrastructure services are configured (deployment automation services, LDAP servers). Only once all the infrastructure is in place will databases and application services be restored.

Function	Category	Contractor Response
🟩	**Improvements (RC.IM):** Recovery planning and processes are improved by incorporating lessons learned into future activities.	Please refer to the response for RC.RP above.
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	Please refer to the response for RC.RP above.