Education Technology Joint Powers Authority

EDUCATION TECHNOLOGY
JOINT POWERS AUTHORITY

RFP No. 23/24-03
Security and IT Administration
PROPOSAL DEADLINE: December 14, 2023, 4:00pm

Contact: Michelle Bennett, Purchasing Dept.
Education Technology JPA
5050 Barranca Parkway, Irvine, California 92604
Telephone: (949) 936-5022 Fax (949) 936-5219
Email: edtechjpa@iusd.org

All dates subject to change at the sole discretion of Ed Tech JPA. Please continue to check our website throughout the proposal and selection periods for updates.

https://edtechjpa.org/procurement/current-procurements

NOTICE CALLING FOR PROPOSALS

AGENCY: Education Technology JPA

PROPOSAL DEADLINE: December 14, 2023 at 4:00 pm

PLACE OF RECEIPT:
Education Technology JPA
%: Irvine Unified School District
Purchasing Department
Attn: Michelle Bennett
5050 Barranca Parkway
Irvine, California 92604-4652

NOTICE IS HEREBY GIVEN that the Education Technology JPA, acting by and through its Governing Board, hereinafter referred to as "Ed Tech JPA" will receive up to, but no later than, the above stated Proposal Submission Deadline, sealed Proposals at the place identified above for its upcoming RFP No. 23/24-03 Security and IT Administration.

Request for Proposal documents can be downloaded at:
https://edtechjpa.org/procurement/current-procurements .

Time is of the essence. The Ed Tech JPA reserves the right to reject any and all submissions, to negotiate with any or all responsible Proposers, and to waive any deficiencies, irregularities or informalities in any proposal or during the evaluation process. The award of a Master Contract(s), if made by the Ed Tech JPA, will be by action of the Governing Board.

Pre-Proposal Vendor Conference: The Ed Tech JPA will conduct a non-mandatory pre-proposal vendor conference on September 28, 2023 at 12:00pm pacific time at https://iusd.zoom.us/j/86856598342?pwd=SGNzNEJaRHd4R2V0V25jSVBSeEU4UT09, Meeting ID: 868 5659 8342, Passcode: cxdmU6. Vendors who wish to attend this meeting should RSVP to edtechjpa@iusd.org.

Any questions regarding the Request for Proposals shall be directed to edtechjpa@iusd.org, via e-mail only by 12:00 pm on December 5, 2023. All responses will be posted on the Ed Tech JPA's website.

Education Technology JPA
Governing Board

Publish: September 15 & 22, 2023

Table of Contents

1.0 Background and Overview

1.1 Overview

The Ed Tech JPA, a California Joint Powers Authority (Ed Tech JPA), invites qualified, experienced vendors (Vendors) to submit responsive proposals (Responses, Proposals, or Proposal Forms) in compliance with the specifications contained in this Request for Proposals (RFP). This RFP is for security and IT administration products, although ancillary services may be included in the provision of these items. Installation services may be requested via this RFP. Selection for award(s), if any, will go to the Vendor(s) who submit Responses that Ed Tech JPA determines to be most advantageous to Ed Tech JPA and the entities it represents. **Products offered by the Vendor(s) selected for the award of a Master Agreement will be available for purchase by all California public agencies and public agencies outside of California who have verified that they are eligible to participate.**

In addition to reviewing proposals for Ed Tech JPA, the initiating agency, Irvine Unified School District, has an immediate need for security, classroom management, help desk and project management solutions. The initiating district will review proposals to determine a Vendor best suited to provide the product for its own needs and anticipates entering into a Purchase Agreement for the product following execution of the Master Agreement awarded pursuant to this RFP.

1.2 Joint Powers Authorities

Pursuant to the California Joint Exercise of Powers Act, a JPA may be created in California when two or more local government entities enter into an agreement to exercise jointly any power common to the contracting parties. JPAs are frequently used to aggregate expertise and purchasing power for procurement, as in the case of insurance or utilities services. JPAs can be given any of the powers inherent in the participating members, as specified in a joint powers agreement.

1.3 Ed Tech JPA

Ed Tech JPA is a JPA duly formed and existing under the California Joint Exercise of Powers Act. Ed Tech JPA was formed to aggregate purchasing power and expertise for public agencies. While Ed Tech JPA's focus is primarily California K-12 public schools, our membership has grown to include colleges and government agencies outside of California. This RFP is issued on behalf of Ed Tech JPA's membership. A list of current Ed Tech JPA members is available on the JPA's website: https://edtechjpa.org/about/our-ed-tech-jpa-members .

1.4 Requested Services

This solicitation is intended to provide a mechanism for Ed Tech JPA members ("Members") to procure new or upgraded security and IT administration products to support their needs. Members seek state-of-the-art security and IT administration products (hereinafter referred to as "Product" or "Solution") to meet the needs of varied facilities and programs, in a variety of environments. Ed Tech JPA is soliciting qualified service vendors, (hereinafter referred to as "Vendor", "Contractor" or "Provider") for a variety of solutions to meet its Members' needs. Vendor shall submit a proposal for the purchase, implementation and ongoing services for security and/or IT administration products.

1.5 Eligible Entities and Participants

The pricing, terms, and conditions of any award pursuant to this RFP will be made available to current Ed Tech JPA members and to other "Eligible Entities" who elect to join the Ed Tech JPA. For purposes of this RFP, Eligible Entities are: (a) all California public school districts, county offices of education, and community college districts, and (b) any other public agency in the United States whose procurement rules, whether internal rules or rules enacted pursuant to statute, allow them to purchase goods or services through a procurement vehicle such as Ed Tech JPA.

For purposes of this RFP, a “Participant” or “Enterprise” is an Eligible Entity who chooses to purchase items through this RFP. Eligible Entities must first become Associate Members of the JPA by entering into an Associate Member Agreement, and thereafter may elect to become Participants of a Master Agreement by entering into a Purchase Agreement with a vendor. Founding Members of Ed Tech JPA may be a Participant without entering into an Associate Member Agreement.

Notwithstanding the purchase anticipated by the initiating district stated above, an award issued pursuant to this RFP does not represent an obligation by Ed Tech JPA, or by any Eligible Entity, to purchase items. Although a Master Agreement awarded under this RFP does not guarantee a particular level of sales as a result of that Master Agreement, Ed Tech JPA’s mission to meet the procurement needs of our program Participants indicates that a Vendor who is committed to this program will achieve success in its sales efforts.

1.6 Master Agreement

Pursuant to Public Contracts Code 20118.2 and Government Code 6500 and 6502, Ed Tech JPA (on behalf of membership) is issuing this RFP for the Products. Vendors offering special services pursuant to Government Code 53060 may also respond to this RFP. Ed Tech JPA will evaluate proposals and all vendors that meet minimum criteria/score and agree to required terms will enter into a Master Agreement with Ed Tech JPA, setting forth the general terms for purchase of the Solution. A sample Master Agreement is attached in Appendix A.

After a Master Agreement has been established, the Vendor’s proposed Solution will be listed on the Ed Tech JPA website. Ed Tech JPA will also include procurement instructions and contract documentation for Founding Members and Associate Members on its website. Details of the procurement process and administrative fee payment will be provided to Vendor finalists upon award. All participating Vendors must comply with Members’ needs and Ed Tech JPA’s processes to ensure compatibility with all legal and regulatory requirements.

Each Participant is responsible for completing their own due diligence regarding the suitability of Vendor, including using price as a significant factor.

Awarded Vendors will work with Ed Tech JPA to negotiate a Purchase Agreement to be executed when a Participant elects to purchase the Solution. Prior to executing a Purchase Agreement with a Participant, Vendor will establish an implementation timeline and implementation plan specific to the Participant’s needs, as further described in Section 2. An Eligible Entity is not bound to a purchase until it has obtained any necessary approval from its Board and executed a Purchase Agreement with the Vendor for the Solution.

Vendors must report to Ed Tech JPA any income directly or indirectly resulting from the sale of products included in the Master Agreement to Participants, for purchases made using Ed Tech JPA agreements and/or relying on this RFP excluding renewals of pre-existing contracts. Reports must be submitted for the Quarters and within the timeline outlined in section 1.14 of this RFP and in section 14.C. of the sample Master Agreement attached hereto as Appendix A. Vendors must remit a copy of all Purchase Agreements, including renewals and amendments, to Ed Tech JPA within 30 days of request by Ed Tech JPA. Vendors participating in this RFP agree to a standing audit by the Ed Tech JPA for all products included in the Master Agreement.

1.7 Period of Performance

The term of the Master Agreement resulting from this RFP shall be five (5) years. Purchase Agreements entered into by Participants and Vendor shall be subject to a maximum contract length of five (5) years, or may be shorter, as the parties elect. The Master Agreement may be terminated by Ed Tech JPA for convenience after three (3) years by the giving of notice of at least thirty (30) days before the expiration of the three (3) year term.

The parties understand that Participants ordering Products pursuant to the Master Agreement may extend for multiple years after the Term of the Master Agreement. The expiration or termination of the Master Agreement shall not affect Vendor's obligation to deliver Products ordered by Participants prior to the expiration of the Master Agreement.

1.8 Reservation of Rights

Ed Tech JPA reserves the right to award all, none, or select portions of this RFP to one or multiple vendors. Ed Tech JPA reserves the right to negotiate terms and conditions of the RFP as necessary, to reject any or all proposals, to increase quantities, and to waive any irregularities or informalities in the RFP or in this process.

Ed Tech JPA reserves the right to modify the RFP documents, or any portion thereof, by the issuance of written addenda posted on the Ed Tech JPA website. In the event Ed Tech JPA shall modify any portion of the RFP documents pursuant to the foregoing, the proposal submitted by any Vendor shall be deemed to include any and all modifications reflected in any addenda issued.

Ed Tech JPA reserves the right to conduct a background inquiry of the selected Vendor(s) which may include collection of contractual and business associations and practices, employment histories and reputation in the business community. By submitting a proposal, Vendor consents to such an inquiry and agrees to make available such books and records deemed necessary to conduct the inquiry.

Ed Tech JPA reserves the right to award multiple Master Agreements for each classification of Products listed in this RFP as deemed to be in the best interest of Ed Tech JPA and its Members and has determined that awards to more than one Vendor for comparable goods and services at various prices may best meet the needs of Participants.

Ed Tech JPA shall have the right to negotiate any and all of the final terms and conditions of any agreement with Vendor and nothing in this RFP or any Response shall be deemed or construed as a limitation of such rights.

This RFP is solely a solicitation for Proposals. Neither this RFP, nor any response to this RFP shall be deemed or construed to: (i) create any contractual relationship between Ed Tech JPA and any Vendor; (ii) create any obligation for Ed Tech JPA or its Members to enter into a contract with any vendor or other party; or (iii) serve as the basis for a claim for reimbursement for costs associated with submittal of any Proposal.

PROVISIONS REQUIRED BY LAW: Vendor acknowledges that it has conducted and performed the required research to become aware and knowledgeable of all federal, state and local laws/statutes that are referenced herein, may pertain to and/or govern the procurement activities and transactions covered by this RFP. These provisions of law and any clause required by law that is associated with and relates to this RFP and any resulting contract will be read and enforced as though it were included herein.

1.9 Data Privacy Compliance

Vendors' Products and services must be fully compliant with all applicable requirements including all state and federal laws. Vendors who would have access to Participant student data will be required to execute the most recent version of the Standard Student Data Privacy Agreement CA-NDPA (CA-NDPA). A copy of the CA-NDPA is attached hereto in Appendix F.

1.10 Indemnification

Vendor will indemnify, defend and hold harmless Ed Tech JPA, its agents, employees and assigns, including independent contractors, and any Participant contracting with Vendor (Indemnified Parties) from any and all claims, demands, suits, proceedings, loss, cost and damages of every kind and description, including any attorney's fees and/or litigation expenses, which might be brought or made against or incurred by Indemnified Parties on account of loss or damage to any property or for injuries to or death of any person, caused by, arising out of, or contributed to, in whole or in part, by reasons of any act, omission, professional error, fault, mistake, or negligence of Vendor, its employees, agents, representatives, or subcontractors, their employees, agents, or representatives in connection with or incident to this RFP, or arising out of worker's compensation claims, unemployment compensation claims, or unemployment disability compensation claims of employees of the Vendor, and/or its subcontractors or claims under similar such laws or obligations. Vendor's obligation under this section will not extend to any liability caused by the sole negligence of Indemnified Parties.

1.11 Special Note on Vendor Pricing

Vendors may propose a variety of products and services to meet the requirements in the RFP. Vendors may choose to offer products and services individually and/or as part of a bundled option. For example, vendors may offer security incident response services as an hourly rate, or incident response as an included service under a more comprehensive security as a service annual contract. Additionally, vendors may tier pricing or offer differentiated discounts based on quantity of products or licenses purchased, student enrollment, or other criteria as appropriate.

Vendor may add or delete Products and/or update pricing after award if:

A. Deleted Products have been discontinued and are no longer available;
B. Added Products are either a direct replacement or are substantially equivalent to original Products listed in the RFP, Vendor's Proposal, the Master Agreement and/or any Purchase Agreements, or added Products are enriched capabilities, new modules, technology advancements, and/or service categories within the Products that Vendor did not have at the time Vendor's Proposal was submitted;
C. Vendors' costs of production or delivery have substantially increased due to inflation. Product costs may be adjusted to compensate for such increases. The basis for such adjustments shall not exceed the percentage of change in the Consumer Price Index (CPI), for Pacific Cities and U.S. City Average, for the period of August 1 through July 31 of the then current year, in the category All Urban Consumers, Los Angeles-Long Beach-Anaheim, as published in the Department of Labor, Bureau of Labor Statistics Publication. After substantial evidence of an operational cost increase has been presented and analyzed, Ed Tech JPA may make adjustments as deemed by Ed Tech JPA to be reasonable and fair. Any such adjustment shall not result in an increase greater than five percent (5%) annually.
D. The Manufacturer's Suggested Retail Prices (MSRP) has significantly changed during the agreement period. In the event of an increase in MSRP, Vendors' may adjust pricing proportionally to the change. In the event of a price decline, such lower prices are to be immediately extended to JPA Members. In addition, within 24 hours of any price decrease, Ed Tech JPA and applicable Participants shall be notified in writing of such changes and pending orders shall reflect the newer price. Any price increases shall be effective upon the completion of an amendment, not to be delayed by the parties.
E. Vendor receives an executed Amendment to the MA;
F. Vendor receives an executed Amendment to any applicable PA

1.12 Ed Tech JPA Administrative Fee

Vendor agrees to pay Ed Tech JPA an administrative fee (the “Admin Fee”) as stated on the Ed Tech JPA website (https://edtechjpa.org/administrative-fee), calculated as a percentage of the invoiced amount of each Participant agreement with Vendor based on an award under the RFP and all revenue derived directly from any Purchase Agreement, including any additional services, and agreement extensions or renewals.

Computations of the Admin Fee shall exclude state, local, or federal taxes levied on invoiced amounts. Unless otherwise stated herein, the Admin Fee is not refundable to Participants or Vendors under any circumstances. In the event the Ed Tech JPA board of directors determines to modify the Admin Fee or how it is calculated, the changes shall be communicated to Vendors and updated on the website. Such changes shall take effect no sooner than thirty (30) days after notifying Vendor and shall apply to all Purchase Agreements entered into thereafter. The Admin Fee shall not be increased to over four percent (4%). Vendor shall be permitted to amend the Master Agreement pricing in the attached Exhibit A in direct proportion to the adjusted Admin Fee.

1.13 Minimum Price Guarantee

To prevent underpricing and protect seller margin, Vendor’s pricing shall be subject to a Minimum Price Guarantee (MPG), whereby, Vendor shall agree not to sell directly, or through a reseller, the Products(s) subject to the Master Agreement at a price lower than the price offered pursuant to the RFP and the Master Agreement to Ed Tech JPA’s Eligible Entities located in California (regardless of whether the Eligible Entity is a Member of the Ed Tech JPA). Ed Tech JPA may consider exceptions to the Minimum Price Guarantee to continue legacy pricing for existing customers or other compelling business needs.

During the period of delivery under a contract resulting from this RFP, if the price of an item decreases, Ed Tech JPA Participants shall receive a corresponding decrease in prices on the balance of the deliveries for as long as the lower prices are in effect. Vendor agrees to amend the Master Agreement to reflect the decreased pricing. Ed Tech JPA Participants shall be given the benefit of any lower prices which may, for comparable quality and delivery, be given by the Vendor to any other school district or any other state, county, municipal or local government agency in a California county for the product(s) listed in the RFP. At no time shall the prices charged to Ed Tech JPA Participants exceed the prices under which the RFP was awarded.

1.14 Usage Reporting Requirement

Upon contract award pursuant to this RFP, all Vendors will be required to provide quarterly usage reports to Ed Tech JPA or designee. The initiation and submission of the quarterly reports are the responsibility of the Vendor. Ed Tech JPA is not required to provide prompting or notification. Vendor is responsible to collect and report all sales data including resellers and partners sales associated with the Master Agreement. Quarterly reports must coincide with the quarters in the fiscal year as outlined below:

Reporting Period	**Due Date**
January 1 - March 31	April 30
April 1 - June 30	July 15 *to allow for fiscal year end
July 1 - September 30	October 31
October 1 - December 31	January 31

Vendors must identify the person responsible for providing the mandatory usage reports. This contact information must be kept current during the Master Agreement period. Ed Tech JPA must be notified if the contact information changes.

The purpose of the Master Agreement usage-reporting requirement is to aid in Master Agreement management. The specific report content, scope, and formal requirements will be provided to the awarded Vendors during Master Agreement execution. Failure to comply with this requirement may result in Master Agreement cancellation.

2.0 Purchase Agreements, Payments & Order Fulfillment

2.1 Purchase Agreements

Upon contract award pursuant to this RFP, Vendors will work with Ed Tech JPA to prepare Purchase Agreement templates for all products available through their Master Agreement. Ed Tech JPA will make the completed Purchase Agreement template available for Members. Sample Agreements are included in Appendix A.

2.2 Ordering Process

It is Ed Tech JPA's intent to make the procurement of products and services as easy as possible. The following outlines the process by which Participants may utilize Ed Tech JPA:

2.2.1 The Ed Tech JPA website includes each Vendor's contact information as listed in Vendor's Proposal and links to Vendor's Proposal, Pricing Forms, Clarifying Questions, Master Agreement, Standard Student Data Privacy Agreement (CA-NDPA) if applicable, and Purchase Agreement template.

2.2.2 Members may browse products, review RFP Proposals on the Ed Tech JPA's website and conduct their own due diligence, using price as a significant factor, to determine which product best meets their unique needs. JPA Members may approach Vendors directly to request services. If a Member contacts Vendor directly, Vendor must provide a copy of the Purchase Agreement and refer Member to Ed Tech JPA's website.

2.2.3 The Participant shall have the opportunity to work with Vendor to determine the suitability of the product, and will provide Vendor with information regarding the Participant's existing software and hardware environment, the number of students/employees/users anticipated to use the Product and any other information necessary to establish an implementation plan. To enable the Participant to make a timely determination as to suitability, within fourteen (14) days of Participant's contact with Vendor, the selected Vendor shall provide the Participant with a project plan that details the proposed i approach and timeline for product delivery and/or full implementation of the products and services as required by the Participant ("Implementation Plan").

2.2.4 If the Participant elects to confirm the purchase, it shall obtain any required board approval, execute the Purchase Agreement including any required exhibits, issue a Purchase Order directly to Vendor, and submit payment to Vendor in accordance with Participant practices.

2.2.5 Vendor shall provide a copy of the executed Purchase Agreement to Ed Tech JPA upon Ed Tech JPA's request.

2.2.6 Once an executed Purchase Agreement is processed, Participant will work directly with Vendor for order fulfillment. Vendor will deliver products and services directly to the Participant in accordance with the implementation plan.

2.3 Purchase Agreement Implementation Process

Vendor will be required to provide Participants with the Solution(s) following Purchase Agreement execution and issuance of a Purchase Order, as agreed by both Vendor and Participant. Participants will work directly with Vendor to receive the Solution.

2.3.1 Project Timeline

Vendor shall deliver the Product to Participant according to the implementation plan identified by the parties pursuant to Section 2.2 above.

2.3.2 Site Access and Work Hours

If Vendor requires access to any school site, access to each site will be coordinated through the Participant project representative a minimum of five (5) work days in advance. Site access schedule and work plan must be submitted and approved by Participant prior to the Vendor arriving onsite.

2.3.3 DOJ Clearance

All Vendor personnel working on any Participant site shall have attained the proper Department of Justice (DOJ) clearance as required by applicable laws and the Participant policy. Vendor must comply with this requirement and, upon request from Participant, must demonstrate this clearance for all personnel prior to being allowed onsite. Those who are not cleared may not be allowed on the project.

2.3.4 Interpretation of Plans and Documents

The interpretation of the plans, specifications, forms, and all project documentation shall be determined by Participant. It is Vendor's responsibility to verify existing conditions and assumptions. Vendor must verify all such information prior to executing a Purchase Agreement with Participant and issuance of a Purchase Order.

2.4. Subscription-based Licensing, Bundling, Additional Services

Purchases made pursuant to this RFP may include equipment, subscription-based licensing, product bundling, and training, maintenance, installation and other additional services ("Additional Services") as determined between the Vendor and Participants. The cost of Additional Services not reflected in the product purchase price found in Appendix D Pricing Form shall also be subject to the Administrative Fee assessed by Ed Tech JPA.

3.0 Instructions to Vendors

3.1 Proposal Contact and Correspondence

All correspondence related to the RFP must be directed to the following designated Ed Tech JPA RFP contact:

edtechjpa@iusd.org

There will be no verbal understandings recognized by the Ed Tech JPA.

No Vendor should attempt to contact or obtain information regarding this RFP from any other Ed Tech JPA representative.

All official records will be posted on the Ed Tech JPA website:
https://edtechjpa.org/procurement/current-procurements
or sent in writing by the official contact listed on the RFP or Amendments. It is the Vendor's responsibility to monitor the website for changes, updates, revisions and/or uploaded documents.

3.2 Proposal Deadline and Submission

Proposals must be received no later than 4:00 pm PST on December 14, 2023.

Vendor to submit:
(1) Master Bound Hardcopy Proposal in a binder that allows for easy removal of pages.
(1) Additional Bound Hardcopy Proposal in a binder that allows for easy removal of pages.
(1) Electronic Proposal on CD or Flashdrive

Proposals shall be submitted in a sealed box/envelope and shall be clearly marked: "Response to RFP 23/24-03 Security and IT Administration."

Proposals shall be submitted to:
Ed Tech JPA
% Irvine Unified School District
Purchasing Department
Attn: Michelle Bennett
5050 Barranca Parkway
Irvine, California 92604

3.3 Delivery to Ed Tech JPA

Proposals may be delivered between the hours of 9:00am and 4:00pm on weekdays, excluding holidays. Written Proposals must be received at the Ed Tech JPA Procurement Office no later than the Proposal Submission Deadline specified in the Calendar of Events. No telegraphic, facsimile, or emailed Proposal will be accepted. The Ed Tech JPA assumes no responsibility for late delivery.

If discrepancies between two (2) or more copies of the Proposal are found, the Proposal may be rejected. If, however, the Proposal is not rejected, the master copy will provide the basis for resolving such discrepancies.

3.4 Withdrawal, Resubmission or Modification

A Vendor may withdraw the Proposal at any time prior to the Proposal Submission Deadline specified in the Calendar of Events, by submitting a written request for its withdrawal to the designated Ed Tech JPA RFP contact, signed by the Vendor or authorized agent. The Vendor may thereafter submit a new or modified Proposal prior to the Proposal Submission Deadline. Modification offered in any other manner, oral or written, will not be considered. A Proposal cannot be changed, corrected, or withdrawn after the Proposal Submission Deadline.

3.5 Calendar of Events

Event	Details	Date
Advertisements - RFP Posting	OC Register	September 15 & 22, 2023
Pre-Proposal Vendor Conference (Non Mandatory)	https://iusd.zoom.us/j/86856598342?pwd=SGNzNEJaRHd4R2V0V25jSVBSeEU4UT09 Meeting ID: 868 5659 8342 Passcode: cxdmU6 Find your local number: https://iusd.zoom.us/u/ksb5MeVae Meeting ID: 868 5659 8342 Passcode: 828567	September 28, 2023 12:00PM
Last Day to Submit Questions (RFIs)	edtechjpa@iusd.org	December 5, 2023 12:00PM
Response to Questions Posted	Ed Tech JPA website	December 8, 2023
Proposals Due	5050 Barranca Pkwy. Attn: Michelle Bennett Irvine, CA 92604	December 14, 2023 4:00PM
Evaluation and Selection of Finalists		December 15, 2023 - February 21, 2024
Ed Tech JPA Board Action		February 29, 2024 *anticipated

All dates are subject to change. Amendments to these dates, and other aspects of the RFP, will be posted at https://edtechjpa.org/procurement/current-procurements .

In an effort to facilitate award and availability of contracts, Vendors who agree to all terms and conditions in the Agreements and do not have exceptions to the RFP may be awarded on an earlier timeline than vendors requesting redlines and exceptions. Requests redlines and exceptions may result in a delayed award. Requesting redlines will not affect a Vendor's award status, but may delay award and the availability of agreements for Member use. Awards shall be made contingent upon successful contract negotiations as determined by Ed Tech JPA's sole discretion.

3.6 Preparation

A Proposal should be prepared in such a way as to provide a straightforward description of Vendor capabilities to satisfy the requirements of this RFP. Emphasis should be concentrated on conformance to the RFP instructions, responsiveness to the RFP requirements, and completeness and clarity of content.

The completed documents(s) should be without interlineations, alterations, or erasures. The Proposal should present all information in a concise manner, neatly arranged, legible, and in terms understandable for evaluation. All information requested is to be addressed directly and completely. It is more desirable to give additional information than less when the answer could be misinterpreted.

Proposals must follow Ed Tech JPA's prescribed format, including all required forms and response templates. Vendors must include all documents and forms indicated in the Proposal Submission Checklist provided in Appendix B. Write out all answers using the Proposal Form template provided. Additional material may be submitted with the proposal as appendices. No brochures or marketing materials will be considered when scoring Proposals. Cross-references to the Proposal Form in additional materials will not be considered responsive. Any additional descriptive material that is used in support of any information in Vendor's proposal must be clearly identified.

The contents of Vendor's proposal, including technical specifications for hardware and software and software maintenance fees, shall remain valid for a minimum of one hundred and sixty (160) days after the proposal due date. If selected, Vendor's Proposal pricing shall remain valid for the duration of the contract term including the original contract and all extensions. If Vendor's Proposal includes functionality from a different platform than the security and IT administrative services listed the platform offering the functionality shall be clearly identified and all additional costs must be outlined clearly and included in the Optional Costs section of the Pricing Form in Appendix D. Costs not identified by the Vendor shall be borne by the Vendor and will not alter the requirements identified in this solicitation.

The person signing verifies that he/she is authorized to submit the proposal and bind Vendor to provide the products/services listed in the RFP, Proposal and any resulting Master Agreement and Purchase Agreement(s).

3.7 False and Misleading Statements

A Proposal which contains false or misleading statements, or which provides references which do not support an attribute or condition contended by Vendor, may be rejected if, in the opinion of Ed Tech JPA, such information was intended to mislead Ed Tech JPA in its evaluation of the Proposal, and the attribute, which is a condition or capability of a requirement of this RFP.

3.8 Request for Information (RFI)

Vendors are encouraged to ask questions during the open RFI period. All questions shall be in writing and submitted to the listed Ed Tech JPA contact person. Questions must be received by the deadline specified in the Calendar of Events. There shall be no verbal understandings or clarifications recognized by the Ed Tech JPA. All responses shall be in writing by an authorized Ed Tech JPA employee or their designated representative. Responses to all RFIs received will be posted on the Ed Tech JPA Website. It is Vendor's responsibility to monitor the Ed Tech JPA website for RFI Responses, RFP Amendments, changes, updates, revisions and/or uploaded documents.

3.9 Amendments to the RFP

During the RFP period, the Ed Tech JPA may amend the RFP. Amendments to the RFP and/or calendar of events will be posted at
https://edtechjpa.org/procurement/current-procurements .

3.10 Limits of the RFP

Ed Tech JPA reserves the right to reject all proposals and will determine what future action, if any, will be taken.

All costs incurred in the preparation or submission of a proposal shall be entirely the responsibility of the Vendor and shall not be chargeable directly or indirectly to the Ed Tech JPA, its Members, or Eligible Entities.

3.11 Public Records Act

All records, documents, drawings, plans, specifications and other materials submitted by Vendor in its proposal, during the procurement process, and during the course of any work awarded shall become the exclusive property of Ed Tech JPA and may be **deemed public records** and subject to the provisions of the California Public Records Act (Government Code, sections 6250 et seq.). Ed Tech JPA's use and disclosure of its records are governed by this Act. Ed Tech JPA will accept information clearly labeled "TRADE SECRET," "CONFIDENTIAL," or "PROPRIETARY" as determined by the submitting party in accordance with the Act. Ed Tech JPA will endeavor to inform Vendor of any request for the disclosure of such information. Under no circumstances, however, will Ed Tech JPA be responsible or liable to Vendor or any other party for the disclosure of any such labeled information. Vendors that indiscriminately identify all or most of their proposal as exempt from disclosure without justification may, at Ed Tech JPA's discretion, be deemed non-responsive; and such information shall be deemed public records. Ed Tech JPA will not advise as to the nature or content of documents entitled to protection from disclosure under the California Public Records Act, including interpretations of the Act or the definitions of "Trade Secret," "Confidential" or "Proprietary", however pricing documents are not considered proprietary. If litigation is brought under the Public Records Act concerning documents submitted in response to this RFP, Vendor shall indemnify, defend and hold harmless Ed Tech JPA in such litigation. Ed Tech JPA reserves the right to withhold information for review by competitors until after it has completed its evaluation. Information marked as "Trade Secret," "Confidential" or "Proprietary" will be available to Ed Tech JPA Members through a member's-only webpage unless Vendor indicates that such information should not be available to Ed Tech JPA Members who are considering purchasing Product.

4.0 Evaluation and Award

4.1 General Information

Award will be made to the vendor(s) offering an advantageous proposal for security and IT Administration products and related services. Ed Tech JPA shall not be obligated to accept the lowest priced proposal(s), but will make an award(s) in the best interest of its Members after all factors have been evaluated. Ed Tech JPA may make awards to multiple vendors. All proposals received in response to this RFP will receive a fair and impartial evaluation by the Ed Tech JPA. In conducting this evaluation, Ed Tech JPA and Members may obtain and use information, in addition to that contained in the proposals, from any source desired. Customers on each Vendor's reference list may be contacted, as may other customers selected by the Ed Tech JPA and listed by Vendor as a reference.

Ed Tech JPA shall make its evaluation in its sole discretion and its decision to award a Master Agreement(s) shall be final. Thereafter, Members electing to purchase Product pursuant to an awarded Master Agreement shall use their discretion in evaluating and selecting Product. Ed Tech JPA's evaluation of proposals and Master Agreement negotiations, as well as Eligible Entities' selection of vendor, and Purchase Agreement negotiations associated with this Request for Proposals shall be governed by Public Contracts Code section 20118.2 for equipment, software and related services and shall be governed by Government Code section 53060 for Solutions comprised of solely professional services. Vendors submitting Proposals for products that may store or exchange student data must be located in either the United States or in a country where the General Data Protection Regulation (GDPR) governs and must perform the proposed Solution in either the United States or in a country where the General Data Protection Regulation (GDPR) governs. Vendors outside of the United States whose products may have access to student data must agree to the Standard Student Data Privacy Agreement CA-NDPA with no redlines/amendments. Vendors should note that some Members may have board policies and procedures that limit their ability to contract with agencies outside the United States.

Awards shall be made contingent upon successful contract negotiations as determined by Ed Tech JPA's sole discretion. Even after award Ed Tech JPA may or may not proceed in establishing contracts. Execution of contracts is solely at the discretion of Ed Tech JPA. In the event that Ed Tech JPA elects not to establish a contract with a previously awarded vendor Ed Tech JPA's governing board shall vote to revoke the award and the vendor shall be notified.

4.2 Requirements

Vendors must meet all of the essential requirements defined in this RFP applicable to the proposed Solution, including compliance with performance, licensing requirements, ability to deliver specified services, conformance to the terms and conditions of this RFP, meeting mandatory system requirements, performance expectations, contract requirements and general terms. Vendors that do not meet the minimum requirements may be disqualified. All essential requirements in Attachment 1 shall be denoted in green and with two asterisks (**).

4.2.1 Permits and Licenses

Vendor and all of the Vendor's employees or agents shall secure and maintain in force such licenses and permits as are required by law, in connection with the furnishing of materials, articles, or services listed herein. All operations and materials shall be in accordance with all applicable Federal, State, County and City requirements.

4.2.2 Delivery and Installation Requirements

All items shall be F.O.B. Destination to delivery locations specified in the Site Delivery List. Delivery charges, fuel surcharges or any additional costs associated with delivery will not be accepted or paid by Ed Tech JPA or Participants. Actual delivery of products shall be coordinated with Participants. Pallets and boxes must be broken down and disposed of by Vendor.

4.2.3 Fingerprinting

If applicable, all contractors, including subcontractors shall be required to comply with the provisions of Education Code 45125.1 and 45125.2 and Participant Board policies to ensure that no Vendor employees or employees of subcontractors who may come in contact with Participant pupils in the performance of their duties have been convicted of a violent or serious felony as defined in the California Penal Code Section 677.5(c) and 1192.7(c). During the term of the Agreement, the Vendor, including subcontractors, shall comply with the provisions of Education Code Section 45125.1,including fingerprinting when Participant determines that the Vendor's employees or employees of subcontractor will have more than limited contact with Participant pupils. If the Vendor, or its subcontractors, fails or refuses to comply with this provision, such failure or refusal shall be considered sufficient cause for disqualification from further award considerations. If such failure or refusal to comply occurs after the Purchase Agreement is executed, Participant may terminate the Agreement, in whole or in part, with no penalty.

4.3 Scoring, Interviews & Vendor Presentations

Qualifying Vendors will be evaluated on their complete proposal, based on the following considerations:

Vendor Support and Ability to Perform
Technology Requirements

Functionality and Usability
Price

Vendors must meet all essential requirements in the applicable RFP sections to be awarded a Master Agreement pursuant to this RFP. Essential requirements are denoted in green and with two asterisks (**). Vendors must meet essential requirements as follows:

- **Vendor Support and Ability to Perform:** All Vendors must meet all essential requirements.
- **Technology Requirements -**
  - Section 2.1: All Vendors must meet all essential requirements.
  - Section 2.2: Vendors proposing technology equipment or other tangible goods must meet all essential requirements.
  - Sections 2.3-2.6: Vendors proposing software products and related services must meet all essential requirements.
- **Functionality and Usability -** Vendors may choose to respond only to the sections that are relevant to their Solution offering(s). Each section will be awarded separately based on Vendors adherence to the essential requirements of the section and compliance with all other requirements of the RFP.
- **Price -** All Vendors must meet all essential requirements.

Ed Tech JPA reserves the right to 1) conduct in-person interviews and/or require a formal presentation for all or a portion of the responding Vendors, 2) visit one (1) or more of the Vendor's current customer sites, and conduct discussions with responsible representatives who submit proposals determined to be reasonably susceptible of being selected for an award. Discussions may be for the purpose of clarification to assure full understanding of, and responsiveness to, the solicitation requirements. Prior to award, Vendors may be asked to submit best and final offers. Vendors shall be given fair and equal treatment with respect to any opportunity for discussion and written revision of proposals. In conducting discussions, Ed Tech JPA will not disclose information derived from proposals submitted by competing firms.

Ed Tech JPA will make a Notice of Intent to Award to Provider available to all Vendors on its website. The Award of the RFP will be voted on by Ed Tech JPA's Board at a public meeting. Any Vendor protesting the award of a contract to another Vendor must do so, in writing, within five (5) calendar days of the Intent to Award posting. Grounds for a protest include: Ed Tech JPA failed to follow the selection procedures and adhere to requirements specified in the RFP or any addenda or amendments, there has been a violation of conflict of interest as provided in California Government Code Section 87100 et. Seq., or violation of any State or Federal law. Protests will not be accepted on any other grounds. All protests will be handled by a panel comprised of Ed Tech JPA members. Ed Tech JPA will consider only these specific issues as addressed in the written protest. A written response will be directed to the protesting Vendor within five (5) calendar days of the receipt of the protest, advising the decision with regard to the protest and the basis for the decision.

Participants reserve the right to 1) conduct in-person interviews and/or require a formal presentation 2) visit one (1) or more current customer sites, and conduct discussions with all or a portion of the Vendors with a current Master Agreement in place with Ed Tech JPA.

4.4 Contract and Warranties

Following the Award of the Master Agreement pursuant to this RFP, Participants may enter into a Purchase Agreement with a selected Vendor to deliver the proposed Products and services. The resulting agreement shall conform to the terms and conditions set forth in this RFP and Ed Tech JPA's standard Purchase Agreement. Copies of Ed Tech JPA's standard Master Agreement and the Purchase Agreement are included in Appendix A of this document. Vendors should note any exceptions or proposed alterations to conditions and requirements defined in this document and Ed Tech JPA's standard agreements in Vendors' proposal. Any such exceptions or conditions will be negotiated after proposal evaluation. Proposed exceptions must also be addressed by Vendor and agreed upon by Ed Tech JPA during contract negotiations to be effective. Ed Tech JPA may elect not to award and/or to revoke award based on requested exceptions that cannot be agreed upon.

The Selected Vendor will guarantee that the proposed Products and services shall conform in all material respects to Ed Tech JPA's specifications in this RFP and the Selected Vendor's documentation accompanying or referred to in this RFP. Vendor may add or delete products introduced or removed from the market under the following conditions: A) Deleted products have been discontinued and are no longer available; or B) Added products are either a direct replacement for original products listed in the RFP, Vendor's Proposal, the Master Agreement and/or any Purchase Agreements, or added products are enriched capabilities, new modules, technology advancements, and/or service categories within the Solution that Vendor did not have at the time the RFP Proposal was submitted. To modify the Product list Vendor shall finalize an Amendment to both the Master Agreement and any applicable Purchase Agreements, with written approval by both parties.

If a Master Agreement is awarded as a result of this procurement process, all warranties made by the Selected Vendor, including the Vendor's Proposal, this RFP and any attachments, bulletins, supporting documentation, or addenda to the RFP shall be incorporated into the Master Agreement and shall be binding upon the Selected Vendor, both pursuant to the Master Agreement and in the execution of Purchase Agreement(s) with Participants. This RFP, any Addenda issued, the Selected Vendor's Proposal, and all supporting documentation will become a part of the Master Agreement and all subsequent Purchase Agreements. Any Proposal attachments, documents, letters, and materials submitted by the Vendor shall be binding and may be included as part of the Master Agreement and Purchase Agreement. Submission of a successful Proposal is not the end of the contractual process; further negotiation over the Agreement terms and conditions will be necessary.

4.5 Covenant Against Gratuities

Vendor warrants by signing and submitting its Proposal in response to this RFP that no gratuities (in the form of entertainment, gifts, or otherwise) were offered or given by Vendor or any agent or representative of Vendor to any officer or employee of Ed Tech JPA with a view toward securing the contract or securing favorable treatment with respect to any determinations concerning the performance of the contract.

For breach or violation of this warranty, Ed Tech JPA shall have the right to terminate the contract, either in whole or in part, and any loss or damage sustained by the Ed Tech JPA or its Members in procuring on the open market any services which Vendor agreed to supply shall be borne and paid for by Vendor. The rights and remedies of Ed Tech JPA or its Members provided in the clause shall not be exclusive and are in addition to any other rights and remedies provided by law or under the Master Agreement or Purchase Agreement.

4.6 Hardware and Equipment

Vendor shall not provide "Remanufactured Equipment," i.e. equipment that has been factory disassembled to a predetermined standard, then reassembled by using new parts and some used or recycled components. Participants shall be the first user of the equipment. All items furnished under this RFP shall consist of new and original components.

Vendors must be either manufacturers or factory authorized resellers/distributors for brands they are proposing and must be able to show proof of information. For resellers/distributors, a manufacturer's letter(s) shall indicate authorization to market, sell, distribute, warrant, or supply any equipment or services offered by the manufacturer through the Vendor.

Destination will be designated within the boundaries of the Participant. Actual delivery dates should be coordinated with the Participant. All shipments shall be accompanied by a packing slip. Purchase order number shall appear on all packing slips, invoices, and packages. Vendor(s) shall keep sufficient stock of Equipment and service material to ensure prompt delivery and service schedules. There shall be no minimum quantities required in order for the Participants to place orders. Bid all items F.O.B., Participant offices or as directed by the purchase order of said Participant.

Unless otherwise specified, if any equipment is not delivered within sixty (60) days following issuance of a purchase order, or if Vendor delivers any equipment which does not confirm to the specifications, the Participant may, at its option, annul and set aside the Agreement, whether in whole or in part, and make and enter into a new contract with a new provider in accordance with law for furnishing such equipment so agreed to be furnished. Any additional cost or expense incurred by the Participant in the making of such contract and any additional cost of supplying any equipment by reason of the failure of the Vendor, as above stated, shall be paid by such Vendor.

If Vendor fails or neglects to furnish and/or deliver the equipment or services at the prices quoted or at the times and places agreed upon or otherwise fails to comply with the terms and conditions of this RFP and resulting agreements in their entirety, the Participant reserves the right to cancel existing orders of equipment and/or related services affected by such default, annul and set aside the PA, whether in whole or in part, and make and enter into a new contract with a new provider, in accordance with law, for furnishing such equipment so agreed to be furnished. Any additional cost or expense incurred by the Participant in the making of such contract and any additional cost of supplying any equipment by reason of the failure of the Vendor, as above stated, shall be paid by such Vendor.

Vendors are required to immediately notify Ed Tech JPA and applicable Participants when manufacturers have discontinued awarded Solution(s). A replacement will be considered if the proposed replacement is equal to or exceeds the discontinued Solution's specifications, and is offered at an acceptable price to the Participant. Successful Vendors shall provide substantiating information when requesting consideration of a substitution as an equal.

5.0 Rules

The following rules and regulations must be followed by every Vendor and subcontractor doing business with Participants. Failure to comply may result in the removal of Vendor and/or members of Vendor's crew from the job, and possible back charges for Participants' direct costs.

5.1.1 Participants are tobacco free organizations. The use of tobacco or tobacco products is prohibited on any part of the Participant grounds.

5.1.2 Vendor agrees to abide by all applicable city laws, including those relating to hours and noise of construction work. If Vendors want to work other than hours approved by the city, Vendor must get a waiver from the city.

5.1.3 Anyone not directly involved in the scope of work shall not be on the job site, or Participant property. Vendor assumes full responsibility for all parties on the site who are there as a result of their direct or indirect involvement with the Vendor.

5.1.4 No music, i.e. radios, cassettes, CD's, iPods, headphones, or other electronic or acoustic device, etc.

5.1.5 No pets are allowed on Participant property.

5.1.6 Fraternization or other contact with students is strictly forbidden.

5.1.7 Any Vendor working on a site where students are present when Participant has determined that the Vendor's employees or employees of subcontractor will have more than limited contact with Participant pupils must supply the Participant with certification that all employees on the project have been fingerprinted and approved per state law and Participant Board policy. Vendor must agree to abide by all Participating Association Member policies to enforce the safety of students.

5.1.8 The Vendor shall supply Certificate of Insurance coverages, as outlined in the Insurance Requirement Acknowledgement prior to the start of work (Appendix B).

5.1.9 Vendor is required to collect, haul and dispose of all debris, trash and spoilage associated with this project. Vendor shall keep all items secured and maintained in a safe manner until properly disposed of. (Note: this requirement does not apply to purchased equipment that is not accompanied with installation or white-glove services).

5.1.10 Care must be taken to minimize damage to the surrounding work environment. All areas affected by the project are to be restored to a pristine condition. This includes replacement of any damaged property or equipment, painting, woodwork, wood staining, trim, cabinetry, carpentry, masonry and all other areas as needed.

5.1.11 Participant has a **Zero Tolerance Policy** that will be enforced towards negative or questionable conduct or behavior.

5.1.12 While on Participants' property and/or project area there will be **No Fraternizing** by the Vendor's workforce with anyone outside the project's workforce.

5.1.13 Professional and neat appearance of workforce shall be maintained at all times. No offensive, suggestive, or inappropriate attire will be permitted.

5.1.14 Use of foul, slanderous, offensive, discourteous or disrespectful language WILL NOT be tolerated.

5.1.15 "Cruising" or "Loitering" on Participant property or job site is not permitted at any time. Employees or associates of the Vendor when not engaged in official activities as directed by their employer shall leave Participants' property until the next work call.

5.1.16 Vendor or its employees or associates are not allowed to be in any area of the Participants' property that has not been specifically authorized by Participant or its designee without an official and designated escort.

5.1.17 Vendor will remove and replace all furniture and equipment as required. Vendor will liaison with the appropriate designated representative on relocation of any equipment. Note: the greatest care is to be taken in all cases when dealing with Participant equipment. Any damage is at the Vendor's expense. Vendor must notify Participant two (2) days in advance when personal items must be removed or may be affected by the Vendor.

5.1.18 Vendor shall maintain the project area in the highest state of safety and cleanliness. During the work shift the areas will be kept orderly and not allowed to become cluttered or in a state where safety is compromised. At the end of each shift Vendor shall ensure that all project equipment, material and debris is properly stowed and secured, or picked up and disposed of as appropriate.

5.1.19 Vendor will be required, as part of the Master Agreement with Ed Tech JPA to indemnify Ed Tech JPA and related persons under certain circumstances. Vendor is directed to those sections in the Master Agreement.

5.1.20 Vendor will also be required by the Purchase Agreement to indemnify the Participant and related persons under certain circumstances. Vendor is directed to those sections in the Purchase Agreement.

5.1.21 Vendor, when required by law, and at the request of Participant, shall pay prevailing wages.

5.1.22 Based on the installation plan supplied to the Participant for a particular site or sites, the Participant may require the Provider to obtain a payment bond, a performance bond, or both.

5.1.23 Each Member of Ed Tech JPA may have additional Rules, which will be provided to Vendor upon request. Vendor agrees to adhere to the Rules for each Member that it contracts with.

6.0 Proposal Format

All Proposals shall be submitted on the attached Proposal Form, provided as Attachment 1. These instructions prescribe the mandatory Proposal Form and the approach for the development and presentation of Proposal information. Proposal Form instructions must be adhered to, all questions must be answered, and all requested data must be supplied. Vendor response to each of the minimum requirements in this RFP is required. Failure to respond or non-adherence to any minimum requirement in this section may be cause for the Proposal to be rejected.

Vendor shall submit a Proposal Form with all information requested. The Proposal should be as clear, complete, and consistent as possible. Some items in this section request a direct response or supporting information from the Vendor. Other items are written as statements of compliance. Vendor must confirm compliance/conformance to all statements in its response. All sections and subsections must be addressed. All documents requiring Vendor signature shall be executed by a duly authorized representative of Vendor.

In addition to responding to the defined minimum requirements, Ed Tech JPA encourages Vendor to submit information about additional functionality or services not specifically requested in the RFP and documentation to support the claims in the proposal. Vendor's proposal should be constructed to provide a complete picture of the features of the proposed Solution, the Vendor's ability to perform, and functionality or services that may distinguish the proposed Solution from other competitive offerings. Proposals will be evaluated both on the satisfaction of Ed Tech JPA's minimum requirements, as well as the additional information submitted by Vendors to depict their complete Solutions. Additional material may be submitted with the proposal as appendices. No brochures or marketing materials will be considered when scoring Proposals. Any additional descriptive material that is used in support of any information in Vendor's proposal must be clearly identified.

Vendors must meet all essential requirements in each Section completed in Vendor's response to be awarded a Master Agreement for that Section pursuant to this RFP. Essential requirements are

denoted in green and with two asterisks (**). If Vendor does not offer aspects of a solution Vendor may leave the Section asking for details about the Products not offered blank, and make a note “Not Included”.

Appendix A: Standard Master Agreement and Standard Purchase Agreement

ED TECH JPA MASTER AGREEMENT:
RFP No. 23/24-03 Security and IT Administration

This Master Agreement ("MA"), is made as of **DATE** **(**"Effective Date"), by and between the Education Technology Joint Powers Authority ("Ed Tech JPA") and **[INSERT]** ("Vendor").

BACKGROUND

A. Education Technology JPA is a Joint Powers Authority formed by California public agencies pursuant to California Government Code Sections 6500-6536. Ed Tech JPA aggregates purchasing power and expertise for its members ("Members").

B. Ed Tech JPA establishes its contracts for products and services through the following process:

1. On September 15, 2023, Ed Tech JPA issued a Request for Proposal for security and IT Administration (the "RFP") on behalf of Members. Ed Tech JPA invited qualified vendors to submit pricing products and services in response to the RFP.
2. Ed Tech JPA published the RFP on its website and in a local periodical:
3. Ed Tech JPA received one or more responses to the RFP. Ed Tech JPA evaluated all responses which complied with the terms of the RFP, using the following criteria: Functionality and Usability, Vendor Support and Ability to Perform, Price, and Technology Requirements.
4. Ed Tech JPA selected Vendor for an award under the RFP for **security and IT administration** and related services ("Products"). The parties are entering this Master Agreement ("MA") to evidence the terms and conditions of that award.

AGREEMENT

Now, therefore, for good and valuable consideration, the parties agree as follows.

1. GRANT AND ACCEPTANCE OF AWARD

Ed Tech JPA awards this MA to Vendor under the RFP with respect to the Products at the prices listed in Exhibit A. Vendor accepts the award and confirms Vendor's acceptance of all terms and conditions of the RFP, which are incorporated herein by this reference. The RFP, Vendor's proposal in response to the RFP ("Vendor's Proposal"), and the Standard Student Data Privacy Agreement ("NDPA") if applicable, are incorporated herein by this reference. This MA includes the Products and pricing offered in Vendor's Proposal, as identified in the RFP. Prices will remain valid for all Members through the expiration of the MA and for Members with an active Purchase Agreement with Vendor ("Participants") through the expiration of any Purchase Agreements ("PA") entered into directly between Vendor and Participants during the term of this MA.

2. TERM

The term of this MA (the "Term") shall commence on the Effective Date and shall expire after a period of five (5) years. The Agreement may be terminated by Ed Tech JPA or Vendor for convenience after three years by the giving of notice of at least thirty (30) days before the expiration of the (3) year term. The parties understand that Participants may order Products under this MA to be delivered after the Term of this MA; in some cases, Products may be delivered over multiple years after the Term. The expiration or termination of this MA shall not affect Vendor's obligation to deliver Products as ordered by Participants during the Term.

3. PARTICIPANTS

The pricing, terms, and conditions of this MA will be made available to Members and to other “Eligible Entities” who elect to become Members. Eligible Entities are all California public school districts, county offices of education, and community college districts, and any other public agency in the United States whose procurement rules, whether internal rules or rules enacted pursuant to statute, allow them to purchase Products through a procurement vehicle such as Ed Tech JPA.

Vendor acknowledges that each Participant is responsible for (a) completing their own due diligence regarding the suitability of Vendor and Products for Participant’s needs, (b) entering into one or more PAs with Vendor to document the quantities, total fees, and delivery terms for Products, and (c) coordinating implementation of Products with Vendor.

Vendor is not under any contractual obligation to provide Products to Participants until such time as both a MA and a PA have been fully executed. The RFP was conducted for the limited purposes specified in the RFP. Ed Tech JPA does not provide assurance or warranty to Vendor or Participant with respect to other issues, including Participant’s payments to Vendor. Ed Tech JPA will not assist in implementation or represent Vendor in the resolution of disputes with Participants.

4. PURCHASE AGREEMENTS

Members may browse products on the JPA website. Prior to executing a PA, Members will work with a Vendor representative to determine the Vendor implementation timeline and implementation plan ("Implementation Plan") as further described in the RFP. To confirm Participant’s request to buy Products using the RFP, Participant and Vendor must complete and execute a PA for the specific Products. Vendor shall provide a copy of complete PAs to Ed Tech JPA within thirty (30) days of request by Ed Tech JPA.

The PA will contain a general description of the Products ordered, contact information for Vendor and Participant related to purchase and sale of the Products, and an acknowledgement that the purchase is subject to the terms of the RFP and this MA. Participant and Vendor may agree on contingencies, such as timing contingencies, applicable to delivery of Products.

Vendor will work directly with a Participant to fulfill the order according to the parties' agreed-upon Implementation Plan. Ed Tech JPA is not responsible to verify payment to Vendor.

5. PROGRAM PROMOTION

It is in the interest of both parties that Vendor will promote and support this MA using methods that best suit the Vendor’s business model, organization, and market approach. Ed Tech JPA specifically desires Vendor to generate interest in the MA, and direct Eligible Entities who express an interest in making a purchase or renewing use of Products to use its MA as Vendor’s preferred form of contracting.

Vendor may be asked to participate with Ed Tech JPA staff in related trade shows, product demonstrations, conferences, and online presentations to promote the MA. Ed Tech JPA will promote MAs through the creation of marketing materials, as well as active outreach to its Members.

Ed Tech JPA expects Vendor’s field and internal sales forces will be trained and engaged in use of the MA for the duration of the contract term.

Ed Tech JPA may schedule periodic reviews with Vendor to evaluate Vendor’s performance of the commitments outlined in this MA, as well as leads, current projects and projected sales.

6. INVOICING FOR SERVICES

Vendor shall invoice each Participant for Products and Participant shall disburse payment to Vendor upon receipt of the fully executed PA between Participant and Vendor. The PA is between Vendor and Participant. Ed Tech JPA does not guarantee timely payment.

7. PRODUCT ADDITIONS/DELETIONS

Vendor may add or delete Products introduced or removed from the market under the following conditions:

A. Deleted Products have been discontinued and are no longer available;
B. Added Products are either a direct replacement or are substantially equivalent to original Products listed in the RFP, Vendor's Proposal, the MA and/or any PAs, or added Products are enriched capabilities, new modules, technology advancements, and/or service categories within the Products that Vendor did not have at the time Vendor's Proposal was submitted;
C. Vendor receives an executed Amendment to the MA;
D. Vendor receives an executed Amendment to any applicable PA.

8. MINIMUM PRICE GUARANTEE

Vendor agrees not to sell directly, or through a reseller, the Product at a price lower than the price offered in the RFP and this MA to Ed Tech JPA's Eligible Entities located in California (regardless of whether the Eligible Entity is a Member), including all California public school districts, county offices of education, and community college districts, and any other public agency in California whose procurement rules, whether internal rules or rules enacted pursuant to statute, allow them to purchase goods or services through a procurement vehicle such as Ed Tech JPA.

During the period of delivery under a contract resulting from this RFP, if the price of the Product decreases, Members entering into a new PA shall receive a corresponding decrease in prices on the balance of the deliveries for as long as the lower prices are in effect. Vendor agrees to amend the MA to reflect the decreased pricing. At no time shall the prices charged to Members exceed the prices under which the RFP was awarded. Members shall be given the benefit of any lower prices which may, for comparable quality and delivery, be provided by the Vendor to any other school district or any other state, county, municipal or local government agency in a California County for the Products.

Product costs may be adjusted to compensate for inflation. The basis for such adjustments shall not exceed the percentage of change in the Consumer Price Index (CPI), for Pacific Cities and U.S. City Average, for the period of August 1 through July 31 of the then current year, in the category All Urban Consumers, Los Angeles-Long Beach-Anaheim, as published in the Department of Labor, Bureau of Labor Statistics Publication. After substantial evidence of an operational cost increase has been presented and analyzed, Ed Tech JPA may make adjustments as deemed by Ed Tech JPA to be reasonable and fair. Any such adjustment shall not result in an increase greater than five percent (5%) annually.

9. EXPENSES.

Ed Tech JPA shall not be liable to Vendor for any costs or expenses paid or incurred by Vendor in providing Products and Services for Ed Tech JPA or Members.

10. COMPLIANCE WITH APPLICABLE LAW

The Products must meet the approval of the Ed Tech JPA and shall be subject to the Ed Tech JPA's general right of inspection to secure the satisfactory completion thereof. Vendor agrees to comply with all federal, state and local laws, rules, regulations and ordinances that are now or may in the future become applicable to Vendor, Vendor's business, the Products, equipment and personnel engaged in Products covered by this MA or accruing out of the performance of such Products. If Vendor performs any work knowing it to be contrary to such laws, ordinances, rules and regulations, Vendor shall bear all costs. If applicable, Vendor has executed the Standard Student Data Privacy Agreement (NDPA). The parties acknowledge that for the purposes of the CCPA, Vendor will not (a) retain, use or disclose Member data for any purpose other than for the specific purpose of providing the Products specified in the MA and PA, or (b) sell, rent, release, disclose, disseminate, make available, transfer, or otherwise communicate orally, in writing, or by electronic or other means, Member data to another business or third party for monetary or other valuable consideration. Without in any way limiting the foregoing, the parties agree that Vendor is a “Service Provider” under the California Consumer Privacy Act, Cal. Civ. Code § 1798.100, et seq. & § 1798.140(v) and that nothing about the MA, PA, or the Products involves a “selling” or a “sale” of Member data under Cal. Civ. Code §1798.140(t)(1).

In accordance with the Americans with Disabilities Act of 1990 and section 504 of the Rehabilitation Act, all Products provided under this Agreement shall comply to those applicable rules of the Web Content Accessibility Guidelines ("WCAG 2.0") and such iterations of WCAG as may become applicable during the term of this Agreement.

11. PERMITS/LICENSES

Vendor and all Vendor’s employees or agents shall secure and maintain in force such permits and licenses as are required by law in connection with the furnishing of Products pursuant to this MA.

12. INSURANCE

Vendor shall insure Vendor’s activities in connection with the Products under this MA and agrees to carry insurance as specified in the RFP to ensure Vendor’s ability to adhere to the indemnification requirements under this MA.

Any general liability policy provided by Vendor hereunder shall contain an endorsement which applies its coverage to Ed Tech JPA, members of Ed Tech JPA 's board of trustees, and the officers, agents, employees and volunteers of Ed Tech JPA, individually and collectively, as additional insureds, using language as set forth below:

Ed Tech JPA, its Board of Trustees, officers, agents, employees, and volunteers are named as additionally insured on this policy pursuant to written contract, agreement, or memorandum of understanding. Such insurance as is afforded by this policy shall be primary, and any insurance carried by Ed Tech JPA shall be excess and noncontributory.

13. TRANSACTION REPORTING

Vendor will comply with all reasonable requests by Ed Tech JPA for information regarding Vendor’s transactions with Participants, including transmittal of transaction data in electronic format. Vendor will report to Ed Tech JPA all Products ordered by Participants, in reasonable detail (“Quarterly Reports”), no later than the reporting period outlined in this MA. Quarterly Reports will include details related to PAs, including but not limited to: term dates, Vendor name, purchase price, Admin Fee amount, new/renewal purchase. Vendor acknowledges that Ed Tech JPA will track the use of this MA through databases managed by Ed Tech JPA. Vendor agrees that all fully executed PAs will be accurately and timely reported to Ed Tech JPA.

14. ADMINISTRATIVE FEE

A. Vendor agrees to pay Ed Tech JPA an administrative fee (the “Admin Fee”) calculated as four percent (4%) of the invoiced amount of any Participant agreement with Vendor or the then-current Admin Fee, based on an award under the RFP and all revenue derived directly from any PA, including any additional services, and agreement extensions or renewals. Individual Transactions that meet a certain dollar amount will receive a discount and pay Admin Fees as listed on the JPA website at:

https://edtechjpa.org/administrative-fee

An Individual Transaction is defined as the total sale made by Vendor to individual Ed Tech JPA Members for each Ed Tech JPA Agreement within the same Reporting Period/Quarter.

Computations of the Admin Fee shall exclude state, local, or federal taxes levied on invoiced amounts. Unless otherwise stated herein, the Admin Fee is not refundable to Participants or Vendors under any circumstances. In the event the Ed Tech JPA board of directors determines to modify the Admin Fee or how it is calculated, the changes shall be communicated to Vendors and updated on the website. Such changes shall take effect no sooner than thirty (30) days after notifying Vendor and shall apply to all PAs entered into thereafter. The Admin Fee shall not be increased to over four percent (4%). Vendor shall be permitted to amend the MA pricing in the attached Exhibit A in direct proportion to the adjusted Admin Fee.

B. Quarterly Reports shall be reported and Admin Fees shall be payable at the end of each quarter as follows:

Reporting Period	**Due Date**
January 1 - March 31	April 30
April 1 - June 30	July 15 *to allow for fiscal year end
July 1 - September 30	October 31
October 1 - December 31	January 31

C. Vendor must submit a check, payable to Education Technology Joint Powers Authority remitted to:
Ed Tech JPA
℅ Clovis Unified School District
Business Services Department
1450 Herndon Ave
Clovis, CA 93611

D. The Admin Fee shall **not** be included as an adjustment to Vendor’s Proposal and MA pricing.

E. The Admin Fee shall **not** be invoiced or charged to the Participant.

F. Payment of the Admin Fee is due from Vendor to Ed Tech JPA when Vendor submits Quarterly Reports or when Vendor receives payment from Participant(s), whichever is later.

G. Any payments that a Vendor makes to Ed Tech JPA after the due date as indicated in this MA shall accrue interest at a rate of eighteen percent (18%) per annum or the maximum rate permitted by law, whichever is less, until such overdue amount shall have been paid in full. The right to interest on late payments shall not preclude Ed Tech JPA from exercising any of its other rights or remedies pursuant to this agreement or otherwise with regards to Vendor’s failure to make timely remittances.

H. Failure to meet Quarterly Reporting, Admin Fee requirements, and to submit fees on a timely basis shall constitute grounds for suspension of this contract.

15. CONTRACT MANAGEMENT

A. The primary Vendor contract manager for this MA shall be as follows:
Name:

Attn:

Address:

Email:

Phone:

B. The primary Ed Tech JPA contract manager for this MA shall be as follows:
Education Technology JPA
Attn: Michelle Bennett
5050 Barranca Parkway
Irvine, CA 92604
EdTechJPA@iusd.org
949-936-5022

C. Should the contract administrator information change, the changing party will provide written notice to the affected party with the updated information no later than ten (10) business days after the change.

16. INDEMNIFICATION

To the extent permitted under applicable law, Vendor will defend, indemnify and hold harmless Ed Tech JPA and its directors, officers, employees, volunteers, and agents from and against all damages, costs (including reasonable attorneys' fees), judgments and other expenses arising out of or on account of any third party claim: (i) alleging that the Product infringes or misappropriates the proprietary or intellectual property rights of a third party; (ii) that results from the negligence or intentional misconduct of Vendor or its employees or agents; or (iii) that results from any breach by Vendor of any of the representations, warranties or covenants contained herein or in any direct communication and/or agreement between Vendor and any Member; or (iv) any allegation that the Product does not conform to WCAG 2.0.

To the extent permitted under applicable law, Ed Tech JPA will defend, indemnify and hold harmless Vendor and its directors, officers, employees, and agents from and against all damages, costs (including reasonable attorneys' fees), judgments and other expenses arising out of or on account of any third party claim that results from (i) the negligence or intentional misconduct of Ed Tech JPA or its employees or agents or (ii) any breach by Ed Tech JPA of any of the representations, warranties or covenants contained herein.

The Parties subject to a claim or suit under this section shall promptly provide the other notice in the manner specified in Section 21, below.

17. ATTORNEYS' FEES

If any action at law or in equity is brought to enforce or interpret the provisions of this MA, each party shall cover its own attorney's fees.

18. SEVERABILITY

In the event that any provision of this MA is held invalid or unenforceable by a court of competent jurisdiction, no other provision of this MA will be affected by such holding, and all of the remaining provisions of this MA will continue in full force and effect.

19. DEFAULTS

In the event that Vendor defaults in its obligations under this MA, and if such default is not cured within thirty (30) days after notice of the default from Ed Tech JPA to Vendor, then Ed Tech JPA may pursue any available remedies against Vendor including, but not limited to, termination of this MA.

20. GOVERNING LAW AND VENUE

THIS MA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF CALIFORNIA, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS LOCATED IN ORANGE COUNTY, CALIFORNIA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS MA OR THE TRANSACTIONS CONTEMPLATED HEREBY.

PROVISIONS REQUIRED BY LAW: Vendor acknowledges that it has conducted and performed the required research to become aware and knowledgeable of all federal, state and local laws/statutes that are referenced herein, may pertain to and/or govern the procurement activities and transactions covered by this MA. These provisions of law and any clause required by law that is associated with this transaction will be read and enforced as though it were included herein.

21. NOTICES

All notices under this MA must be in writing and will be effective (a) immediately upon delivery in person or by messenger, (b) the next business day after prepaid deposit with a commercial courier or delivery service for next day delivery, (c) when emailed to the receiving party at the receiving party's assigned email address with delivery receipt requested, upon electronic confirmation the transmission has been delivered, or (d) five (5) business days after deposit with the US Postal Service, certified mail, return receipt requested, postage prepaid. All notices must be properly addressed to the addresses set forth on the signature page to this MA, or at such other addresses as either party may subsequently designate by notice.

22. ASSIGNMENT

Neither party may assign its rights and obligations hereunder, either in whole or in part, whether by operation of law or otherwise, without the prior written consent of the other party. Notwithstanding the foregoing, either party may assign this MA in its entirety, without consent of the other party, to its Affiliate or in connection with a merger, acquisition, corporate reorganization, or sale of all or substantially all of its assets not involving a direct competitor of the other party. Subject to the foregoing, this MA shall bind and inure to the benefit of the parties, their respective successors and permitted assigns. An "Affiliate" for purposes of this Section shall mean any entity which directly controls, is under common control with, or is directly or indirectly controlled by the party seeking to assign its rights and obligations hereunder.

23. INDEPENDENT CONTRACTOR

Vendor, in the performance of this MA, shall be and act as an independent contractor. Vendor understands and agrees that it and all of its employees shall not be considered officers, employees or agents of Ed Tech JPA, and are not entitled to benefits of any kind or nature normally provided to employees of Ed Tech JPA and/or to which Ed Tech JPA's employees are normally entitled, including, but not limited to, State Unemployment Compensation or Workers' Compensation. Vendor assumes the full responsibility for the acts and/or omissions of its employees or agents as they relate to the Products to be provided under this MA. Vendor shall assume full responsibility for payment of all federal, state and local taxes or contributions, including unemployment insurance, social security and income taxes with respect to Vendor's employees.

24. FORCE MAJEURE

Neither party shall be deemed to be in violation of this MA if either is prevented from performing any of its obligations hereunder for any reason beyond its reasonable control, including but not limited to acts of God, natural disasters, earthquake, fire, flood, strikes, civil commotion, labor disputes, war, terrorism, infectious disease, and pandemics. If such an event continues for sixty (60) or more days, either party may terminate this MA by providing a written notification and shall not be liable to the other for failure to perform its obligation.

25. COUNTERPARTS

This MA may be signed and delivered in two (2) counterparts, each of which, when so signed and delivered, shall be an original, but such counterparts together shall constitute the one instrument that is the MA, and the MA shall not be binding on any party until all Parties have signed it.

26. AUTHORIZED SIGNATURE

The individual signing this MA warrants that he/she is authorized to do so. The Parties understand and agree that a breach of this warranty shall constitute a breach of the MA and shall entitle the non-breaching party to all appropriate legal and equitable remedies against the breaching party.

27. SURVIVAL

The parties' respective obligations under the following sections of this MA shall survive any termination of this MA: Sections 13 through 21, covering Transaction Reporting, Administrative Fee, Indemnification, Attorneys' Fees, Severability, Defaults, Governing Law, and Notices.

28. EXHIBITS

This MA includes all documents referenced herein, whether attached hereto or otherwise incorporated by reference.

29. ENTIRE AGREEMENT AND ORDER OF PRECEDENCE. This MA, the RFP, Vendor's Proposal, and the NDPA are the entire agreements between the parties and supersede all prior and contemporaneous agreements, proposals or representations, written or oral, concerning its subject matter. No modification, amendment, or waiver of any provision of this MA will be effective unless in writing and signed by both parties. Notwithstanding any language to the contrary therein, no Vendor terms or conditions stated in Vendor 's Proposal, an invoice, or in any other documentation, will be incorporated into or form any part of this MA, and all such terms or conditions will be void. In the event of any conflict or inconsistency among the following documents, the order of precedence shall be: (1) this MA; (2) any exhibit, schedule, or addendum to this MA; (3) the NDPA; (4) the body of the PA; (5) any exhibit, schedule, or addendum to the PA; (6) Vendor's Proposal; and (7) the RFP.

IN WITNESS WHEREOF, the parties have executed this Master Agreement as of the Effective Date.

Education Technology Joint Powers Authority	**VENDOR**
______________________________	______________________________
By: Brianne Ford	By:
Its: President of the Board	Its:
_______________	_______________
Date	Date

Exhibit A

Ed Tech JPA Pricing

ED TECH JPA PURCHASE AGREEMENT:
23/24-03 Security and IT Administration

This Purchase Agreement ("PA"), is made as of DATE ("Effective Date"), by and between the [INSERT MEMBER] ("Participant") and [INSERT] ("Vendor").

BACKGROUND

A. Education Technology Joint Powers Authority ("Ed Tech JPA") is a Joint Powers Authority formed by local public agencies, pursuant to California Government Code Sections 6500-6536. Ed Tech JPA aggregates purchasing power and expertise for its Members across California and public agencies outside of California who have verified that they are eligible to participate.

B. Ed Tech JPA establishes its contracts for products and services through the following process:

1. On September 15, 2023, Ed Tech JPA issued a Request for Proposal for Security and IT Administration (the "RFP") on behalf of Ed Tech JPA members. Ed Tech JPA invited qualified vendors to submit pricing products and services in response to the RFP.
2. Ed Tech JPA published the RFP on its Website and in a local periodical.
3. Ed Tech JPA received one or more responses to the RFP. Ed Tech JPA evaluated all responses which complied with the terms of the RFP, using the following criteria: Functionality and Usability, Vendor Support and Ability to Perform, Price, and Technology Requirements.
4. Ed Tech JPA selected Vendor for an award under the RFP for security and IT administration products and related services (the "Product") and thereafter entered into a Master Agreement (MA) to establish the terms by which Members of the Ed Tech JPA may purchase products from Vendor.

C. Participant has completed its own due diligence regarding the suitability of Vendor and Products for Participant's needs.

D. The parties are entering this PA to establish the terms and conditions of the purchase by Participant pursuant to that MA.

AGREEMENT

Now, therefore, for good and valuable consideration, the parties agree as follows.

1. PARTICIPATION IN MASTER AGREEMENT

This PA is subject to the terms of the RFP and the corresponding MA between Ed Tech JPA and Vendor, which are incorporated herein by this reference. Vendor and Participant agree (a) to the terms and conditions of the RFP and the MA covering the Product, (b) any additions or deletions to Product listed on this PA shall be promptly executed through an amendment to this PA, signed by Vendor and Participant.

Vendor acknowledges that Participant is responsible for (a) completing its own due diligence regarding the suitability of Vendor and Product, (b) prior to executing a PA, Participant worked with a Vendor representative to establish an Implementation Plan with the Participant, as further described in the RFP, (c) Participant is not bound to a purchase until it has obtained any required approvals from its Board and executed this PA, and (d) by entering into one or more PAs with Participant, Vendor agrees to the delivery terms for Products as established in the Implementation Plan and Vendor will faithfully carry out timely implementation of the Products with Participant. Order details, including any additional services, and the parties' implementation plan ("Implementation Plan") are attached hereto as Exhibit A.

Participant acknowledges and agrees that (a) it has performed its own due diligence in selecting the Vendor's Product and its suitability to Participant's needs, including using price as a significant factor, (b) Vendor has provided a suitable Implementation Plan to Participant outlining all necessary dates and Participant needs, and (c) it will pay the costs as quoted by Vendor in the RFP, MA, and Exhibit A of this PA.

2. COMPLIANCE WITH APPLICABLE LAW

A. Vendor agrees to comply with all federal, state, and local laws, rules, regulations, and ordinances that are now or may in the future become applicable to Vendor, Vendor's business, the Product, equipment and personnel engaged in Products covered by this PA or accruing out of the performance of such Products. If Vendor performs any work knowing it to be contrary to such laws, ordinances, rules and regulations, Vendor shall bear all costs. If applicable, Vendor has executed the Standard Student Data Privacy Agreement CA-NDPA (NDPA). The parties acknowledge that for the purposes of the CCPA, Vendor will not (a) retain, use or disclose Participant data for any purpose other than for the specific purpose of providing the Products specified in the PA, or (b) sell, rent, release, disclose, disseminate, make available, transfer, or otherwise communicate orally, in writing, or by electronic or other means, Participant data to another business or third party for monetary or other valuable consideration. Without in any way limiting the foregoing, the parties agree that Vendor is a "Service Provider" under the California Consumer Privacy Act, Cal. Civ. Code § 1798.100, et seq. & § 1798.140(v) and that nothing about the PA or the Products involves a "selling" or a "sale" of Participant data under Cal. Civ. Code §1798.140(t)(1).

B. In accordance with the Americans with Disabilities Act of 1990 and section 504 of the Rehabilitation Act, all Products provided under this Agreement shall comply to those applicable rules of the Web Content Accessibility Guidelines ("WCAG2") and such iterations of WCAG2 as may become applicable during the term of this Agreement.

3. PERMITS/LICENSES

Vendor and all Vendor's employees or agents shall secure and maintain in force such permits and licenses as are required by law in connection with the furnishing of Products pursuant to this PA.

4. INSURANCE

Vendor shall insure Vendor's activities in connection with the Products under this PA and agrees to carry insurance as specified in the RFP to ensure Vendor's ability to adhere to the indemnification requirements under this PA.

Any general liability policy provided by Vendor hereunder shall contain an endorsement which applies its coverage to Participant, members of Participants' board of trustees, and the officers, agents, employees, and volunteers of Participant, individually and collectively, as additional insureds.   Such insurance as is afforded by this policy shall be primary, and any insurance carried by Participant shall be excess and noncontributory.

5. PRODUCT ADDITIONS/DELETIONS

Vendor may add or delete Products introduced or removed from the market under the following conditions:

A. Deleted Products have been discontinued and are no longer available;
B. Added Products are either a direct replacement or is substantially equivalent to original Products listed in the RFP, Vendor's Proposal in response to the RFP ("Vendor's Proposal"), the MA and/or any PAs, or added Products are enriched capabilities, new modules, technology advancements, and/or service categories within the Product that Vendor did not have at the time Vendor's Proposal was submitted;
C. Vendor executes an Amendment to the MA with Ed Tech JPA;
D. Vendor receives an executed Amendment to the PA.

6. INVOICING FOR SERVICES

The RFP number and name shall appear on each purchase order and invoices for all purchases placed under this PA. Unless otherwise agreed upon by both parties in writing, signing a delivery and acceptance certificate constitutes acceptance of the Product and allows Vendor to invoice for the Product. Ed Tech JPA does not guarantee timely payment. The Purchase Agreement is between Vendor and Participant.

The parties acknowledge that (a) all annual recurring fees are due and payable annually for each year of the Term, and (b) all one-time fees are due in full within thirty (30) days of execution of this PA. Consistent with the above, upon execution of this PA and each subsequent year of the Term, Vendor will submit invoices to Participant. Participant shall have thirty (30) days to process purchase orders and, upon receipt of invoice, Participant shall agree to pay all undisputed invoices in full within thirty (30) days of the date of invoice.

7. LICENSING
Subject to this PA, Vendor hereby grants Participant (including Participant's students, employees, volunteers, parents and authorized guardians of Participant's students, all as applicable and described in the relevant description of services ("Users")), a limited, nonexclusive, nontransferable, non-sublicensable license to access and use the Product during the Term in accordance with applicable laws and regulations.

Except as expressly permitted in this PA, Participant will not itself, and will not authorize or allow any third party to: (a) provide access to the Product to any person who is not a User; (b) reverse engineer, decompile, disassemble or otherwise attempt to discover the source code, object code or underlying structure, ideas or algorithms of the Product; (c) modify, translate or create derivative works based on the Product; (d) copy, rent, lease, distribute, pledge, assign or otherwise transfer or allow any lien, security interest or other encumbrance on the Product; (e) use the Product for timesharing or service bureau purposes or otherwise for the benefit of a third party; (f) hack, manipulate, interfere with or disrupt the integrity or performance of or otherwise attempt to gain unauthorized access to the Product or its related systems, hardware or networks or any content or technology incorporated in any of the foregoing; or (g) remove or obscure any proprietary notices or labels of Vendor or its suppliers on the Product or on any printed or digital materials provided by Vendor.

Participant will itself and will instruct its Users to: (i) attempt to prevent unauthorized access to or use of the Product; and (iii) notify Vendor promptly of any known or suspected unauthorized access or use. Participant will reasonably assist Vendor in all efforts to investigate and mitigate the effects of any such incident. Upon expiration or any termination for any reason of the Agreement, (i) all rights granted to Participant will immediately terminate and Participant will promptly cease use of the Product, (ii) Vendor will grant Participant a three (3) month period to export Participant data from the Product, (iii) Vendor has no obligation to maintain or provide any Participant data after the termination or expiration of this PA.

8. LIMITATIONS OF LIABILITY
Disclaimer of Consequential Damages. THE PARTIES HERETO AGREE THAT, NOTWITHSTANDING ANY OTHER PROVISION IN THIS PA OR ANY ASSOCIATED AGREEMENT, EXCEPT FOR LIABILITY ARISING OUT OF THE PARTIES' INDEMNIFICATION OBLIGATIONS SET FORTH IN THIS PA, AS APPLICABLE, IN NO EVENT WILL EITHER PARTY BE LIABLE TO THE OTHER FOR ANY SPECIAL, INDIRECT, RELIANCE, INCIDENTAL OR CONSEQUENTIAL DAMAGES OF ANY KIND, LOST PROFITS OR LOST REVENUE, WHETHER ARISING IN CONTRACT, TORT (INCLUDING NEGLIGENCE), OR OTHERWISE, EVEN IF A PARTY HAS BEEN NOTIFIED OF THE POSSIBILITY THEREOF.

General Cap on Liability. NOTWITHSTANDING ANY OTHER PROVISION OF THIS AGREEMENT OR ANY ASSOCIATED AGREEMENT, EXCEPT FOR LIABILITY ARISING OUT OF (A) PARTICIPANT'S USE OF THE PLATFORM OTHER THAN EXPRESSLY PERMITTED BY THIS PA AND FAILURE TO CURE THEREIN AS SPECIFIED AND (B) THE PARTIES' INDEMNIFICATION OBLIGATIONS SET FORTH IN THIS PA, AS

APPLICABLE, UNDER NO CIRCUMSTANCES WILL EITHER PARTY'S LIABILITY FOR ALL CLAIMS OF PARTICIPANT ARISING UNDER OR RELATING TO THIS AGREEMENT (INCLUDING BUT NOT LIMITED TO WARRANTY CLAIMS), REGARDLESS OF THE FORUM AND REGARDLESS OF WHETHER ANY ACTION OR CLAIM IS BASED ON CONTRACT, TORT OR OTHERWISE, EXCEED THE AGGREGATE FEES PAID BY PARTICIPANT TO VENDOR UNDER THIS AGREEMENT. NOTWITHSTANDING ANYTHING CONTAINED IN THIS AGREEMENT OR ANY ASSOCIATED AGREEMENT, VENDOR'S LIABILITY FOR ALL CLAIMS RELATING TO DATA SECURITY OR PRIVACY, REGARDLESS OF WHETHER ANY ACTION OR CLAIM IS BASED ON CONTRACT, TORT OR OTHERWISE, SHALL NOT EXCEED TWO TIMES THE AGGREGATE FEES PAID BY PARTICIPANT TO VENDOR UNDER THIS AGREEMENT DURING THE TWELVE (12) MONTH PERIOD PRECEDING THE EVENT OR CIRCUMSTANCES GIVING RISE TO SUCH LIABILITY. THIS LIMITATION OF LIABILITY IS CUMULATIVE AND NOT PER INCIDENT.

9. INDEMNIFICATION

A. Vendor will defend, indemnify and hold harmless Participant and Ed Tech JPA and their directors, officers, employees, and agents from and against all damages, costs (including reasonable attorneys' fees), judgments and other expenses arising out of or on account of any third party claim:

(i) alleging that the product infringes or misappropriates the proprietary or intellectual property rights of such third party, except to the extent that such infringement results from (A) Participant's misuse of the product, (B) Participant modifications to the product, or (C) Participant continuing the allegedly infringing activity after Vendor has provided Participant with modifications that would have avoided the alleged infringement; (ii) that results from the negligence or intentional misconduct of Vendor or its employees or agents; (iii) that results from any breach of any of the representations, warranties or covenants contained herein by Vendor; (iv) related to a data breach and/or personal injury due to Vendor's recklessness, gross negligence, or intentional conduct; or (v) Resulting from or related to any injury to or death of any person(s), or damage, loss or theft of any property caused by any act, neglect, default or omission of the Vendor or any person, firm, or corporation employed by the Vendor, either directly or by independent contract, arising out of, or in any way connected with the work covered by this PA, whether said injury or damage occurs either on or off Participant property, if the liability arose due to the negligence or willful misconduct of anyone employed by the Vendor, either directly or by independent contract. If the Product becomes or, in Vendor's opinion, is reasonably likely to become the subject of any injunction preventing use as contemplated herein for the reasons stated in this Section, Vendor, or its designee, will either, (i) procure for Participant the right to continue using the Product, (ii) replace or modify the Product so that it becomes non-infringing without substantially compromising its functionality, or, if (i) and (ii) are not reasonably available to Vendor, then (iii) terminate this PA as to the infringing Product, require the return of the allegedly infringing Product and refund to Participant a portion of the fees paid by Participant in respect of the Product depreciated on a straight-line basis over one (1) year from the Effective Date.

Vendor agrees to notify Ed Tech JPA and Participant in the event of any claim against Vendor regarding Products and services listed in the RFP. Vendor agrees to notify Ed Tech JPA of any claims against Vendor by any Participant.

B. To the extent permitted under applicable law, Participant agrees to defend, indemnify and hold harmless Vendor and Ed Tech JPA and their directors, officers, employees, and agents from and against all damages, costs (including reasonable attorneys' fees), judgments and other expenses arising out of or on account of any third party claim that results from (i) the negligence or intentional misconduct of Participant or its employees or agents or (ii) any breach of any of the representations, warranties or covenants contained herein by Participant.

C. Ed Tech JPA does not provide assurance or warranty to Vendor or Participant with respect to issues arising under this PA, including Participant's payments to Vendor. Ed Tech JPA will not represent Vendor or Participant in the resolution of disputes arising under this PA.

10. ATTORNEYS' FEES

If any action at law or in equity is brought to enforce or interpret the provisions of this PA, each party shall pay their own attorneys' fees.

11. SEVERABILITY

In the event that any provision of this PA is held invalid or unenforceable by a court of competent jurisdiction, no other provision of this PA will be affected by such holding, and all of the remaining provisions of this PA will continue in full force and effect.

12. TERM & TERMINATION

The term of this PA (the "Term") shall commence on the Effective Date and shall expire after a period of number (#) years. The parties understand that this PA and subsequent extensions may extend for multiple years after the Term of the Master Agreement, upon mutual written consent of both parties, for a term not to exceed five years. The expiration or termination of the MA shall not affect Vendor's obligation to deliver Products as ordered by Participant pursuant to this PA.

Either Party may terminate this PA upon giving of written notice of intention to terminate for cause. Cause shall include: (a) material violation of this PA or the NDPA by the other party; or (b) any act by Vendor exposing the Participant to liability to others for personal injury or property damage; (c) either party is adjudged a bankrupt, makes a general assignment for the benefit of creditors or a receiver is appointed on account of the party's insolvency or (d) student data breach. Written notice by the terminating party shall contain the reasons for such intention to terminate and unless within thirty (30) days after service of such notice the condition or violation shall cease, or satisfactory arrangements for the correction thereof be made ("Cure Period"), this PA shall, upon the expiration of the Cure Period, cease and terminate. In the event of such termination initiated by Participant due to Vendor's action Vendor shall refund any pre-paid fees to Participant on a prorated basis. The foregoing provisions are in addition to and not a limitation of any other rights or remedies available to Participant. Such termination shall be without any obligation or liability to Vendor other than payment of charges for the value of work performed, and for necessary expenditures which can be established by Vendor as having been reasonably incurred prior to the time that notice of termination is given. In no event shall the termination charges exceed the purchase price of the equipment/services. In the event of any termination, Participant shall be entitled to all materials, work in progress, and completed work included as value of work performed and necessary expenditures in determining the charges referred to above and paid by Participant.

Vendor agrees to allow termination of this PA in whole or in part, in the event that Participant does not allocate funding for the continuation of this contract or any portion thereof. In the event of termination due to non-allocation of funds, both parties shall be held without fault and there shall be no financial consequences assessed as a penalty on either party.

13. GOVERNING LAW AND VENUE

THIS PA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF CALIFORNIA, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS IN THE COUNTY WHERE PARTICIPANT IS LOCATED FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS PA OR THE TRANSACTIONS CONTEMPLATED HEREBY.

PROVISIONS REQUIRED BY LAW: Vendor acknowledges that it has conducted and performed the required research to become aware and knowledgeable of all federal, state, and local laws/statutes that are referenced herein, may pertain to and/or govern the procurement activities and transactions covered by this PA. These provisions of law and any clause required by law that is associated with this transaction will be read and enforced as though it were included herein.

14. NOTICES

All notices under this PA must be in writing and will be effective (a) immediately upon delivery in person or by messenger, (b) the next business day after prepaid deposit with a commercial courier or delivery service for next day delivery, (c) when emailed to the receiving party at the receiving party's assigned email address with delivery receipt requested, upon electronic confirmation the transmission has been delivered, or (e) five (5) business days after deposit with the US Postal Service, certified mail, return receipt requested, postage prepaid. All notices must be properly addressed to the addresses set forth on the signature page to this PA, or at such other addresses as either party may subsequently designate by notice.

A. The primary Vendor contract manager for this PA shall be as follows:

Name:

Attn:

Address:

Email:

Phone:

B. The primary Participant contract manager for this PA shall be as follows:

Name:

Attn:

Address:

Email:

Phone:

C. The primary Ed Tech JPA contract manager for this PA shall be as follows:

Education Technology JPA
Attn: Michelle Bennett
5050 Barranca Parkway
Irvine, CA 92604
edtechjpa@iusd.org
949-936-5022

D. Should the contract administrator information change, the changing party will provide written notice to the affected parties with the updated information no later than ten (10) business days after the change.

15. ASSIGNMENT

Neither party may assign its rights and obligations hereunder, either in whole or in part, whether by operation of law or otherwise, without the prior written consent of the other party, which shall not be unreasonably withheld. Notwithstanding the foregoing, either party may assign this Agreement in its entirety (including all Implementation Plans), without consent of the other party, to its Affiliate or in connection with a merger, acquisition, corporate reorganization, or sale of all or substantially all of its assets not involving a direct competitor of the other party. Subject to the foregoing, this PA shall bind and inure to the benefit of the parties, their respective successors and permitted assigns. An "Affiliate" for purposes of this Section shall mean any entity which directly controls, is under common control with, or is directly or indirectly controlled by the party seeking to assign its rights and obligations hereunder.

16. COUNTERPARTS

This PA may be signed and delivered in two (2) counterparts, each of which, when so signed and delivered, shall be an original, but such counterparts together shall constitute the one instrument that is the PA, and the PA shall not be binding on any party until all Parties have signed it.

17. AUTHORIZED SIGNATURE

The individual signing this PA warrants that he/she is authorized to do so. The Parties understand and agree that a breach of this warranty shall constitute a breach of the PA and shall entitle the non-breaching party to all appropriate legal and equitable remedies against the breaching party.

18. WARRANTY

Vendor represents to Participant that the Product will substantially perform in all material respects the functions described in Vendor's Proposal when used and/or accessed in accordance with the terms and conditions of this PA.

Participant's sole and exclusive remedy for a breach of this warranty shall be: (1) Vendor shall be required to use commercially reasonable efforts to provide modifications or fixes with respect to the applicable nonconformity in the operation of the Product; or (2) in the event Vendor is unable to correct such deficiencies after good-faith efforts, Vendor shall refund any pre-paid fees to Participant on a prorated basis from the date Vendor received such notice. To receive warranty remedies, Participant must promptly report deficiencies in writing to Vendor within thirty (30) days after the deficiency is identified by Participant. The foregoing warranties shall not apply in the event : (i) Participant or its Users use and/or access the Product in a manner which is not in conformance with the terms and conditions of this PA; (ii) Participant or its Users use the Product with third party data, software or hardware which is incompatible with the Product; (iii) errors in the Product are a result of Participant's or its Users' configuration or manipulation of the Product, in each case specifically not recommended in writing by Vendor; or (iv) reduced performance or non-availability of the Product result from failure of network connections, or other factors, beyond the reasonable control of Vendor.

Vendor will use commercially reasonable efforts to make the Product available with an annual uptime percentage of at least 99% ("Service Commitment") after the Product has been fully implemented. In the event Vendor does not meet the Service Commitment, Participant will be eligible to receive a service credit as described herein. The maximum amount of the credit is one twelfth (1/12) of the annual subscription fee for a twelve (12) month period. The service credit is calculated by taking the number of hours the Product was unavailable below the Service Commitment, and multiplying it by three percent (3%) of one twelfth (1/12) the annual subscription fee. If the Participant has been using the Product for less than one year, the preceding one year will be used with any days prior to Participant's use of the Product deemed to have had 100% availability. Any unavailability occurring prior to a credit cannot be used for any future claims. The Service Commitment does not apply to any scheduled outages, standard maintenance windows, force majeure, and outages that result from any technology issue not originating from Vendor. Any service credit shall be calculated using solely the fees paid for the Product. Participant's sole and exclusive remedy for breach of the Service Commitment in this Section will be for Vendor to provide a credit as provided in this Section; provided that Participant notifies Vendor in writing of such claim within thirty (30) days of becoming eligible for such claim.

19. Equipment/Hardware

All equipment shall be new equipment and not remanufactured equipment.

The equipment shall be delivered only after the issuance of a purchase order(s) against the Agreement by the Participant, and shall be delivered F.O.B. to delivery locations specified by Participant in the quantities specified on the purchase order(s). Delivery charges, fuel surcharges or any additional costs associated with delivery only be accepted by Participants as agreed upon in the Quote affixed hereto as Exhibit A. Actual delivery of products shall be coordinated with Participants. Pallets and boxes must be broken down and disposed of by Vendor.Vendor assumes all risk of loss or damage until the equipment has been delivered and accepted by Participant staff at the Participant's approved location. Purchase orders will be issued a reasonable time in advance of the date of delivery. All equipment furnished shall be subject to inspection and rejection by Participant for defects or non-compliance with the specifications. The cost of inspection and/or return shipping for equipment which do not meet the specifications will be borne by the Vendor. Vendor shall replace returned equipment with satisfactory items at no additional cost.

Taxes, delivery charges, fuel surcharges and any additional costs must be included on the Quote affixed hereto as Exhibit A. Actual delivery of products shall be coordinated with Participants. Pallets and boxes must be broken down and disposed of by Vendor at no additional cost.

Unless otherwise specified, if any equipment is not delivered within sixty (60) days following issuance of a purchase order, or if Vendor delivers any equipment which does not confirm to the specifications, the Participant may, at its option, annul and set aside the PA, whether in whole or in part, and make and enter into a new contract with a new provider in accordance with law for furnishing such equipment so agreed to be furnished. Any additional cost or expense incurred by the Participant in the making of such contract and any additional cost of supplying any equipment by reason of the failure of the Vendor, as above stated, shall be paid by such Vendor.

20. SURVIVAL

The parties' respective obligations under the following sections of this PA shall survive any termination of this PA: Sections 9 through 14, covering Indemnification, Attorneys' Fees, Severability, Term & Termination, Governing Law, and Notices.

21. EXHIBITS

This PA includes all documents referenced herein, whether attached hereto or otherwise incorporated by reference.

22. ENTIRE AGREEMENT AND ORDER OF PRECEDENCE.

The RFP, Vendor's Proposal in response to the RFP, the MA, the NDPA (if applicable) and this PA are the entire agreement between the parties and supersede all prior and contemporaneous agreements, proposals, or representations, written or oral, concerning its subject matter. No modification, amendment, or waiver of any provision of this PA will be effective unless in writing and signed by both parties. Notwithstanding any language to the contrary therein, no Vendor terms or conditions stated in Vendor's Proposal, an invoice, or in any other documentation, will be incorporated into or form any part of this PA, and all such terms or conditions will be void. In the event of any conflict or inconsistency among the following documents, the order of precedence shall be: (1) the MA; (2) any exhibit, schedule, or addendum to the MA; (3) the NDPA (if applicable); (4) the body of this PA; (5) any exhibit, schedule, or addendum to this PA; (6) Vendor's Proposal; and (7) the RFP.

23. INDEPENDENT CONTRACTOR

Vendor, in the performance of this PA, shall be and function as an independent contractor. Vendor understands and agrees that it and all of its employees shall not be considered officers, employees, or agents of the Participant, and are not entitled to benefits of any kind or nature normally provided employees of the Participant and/or to which Participant's employees are normally entitled, including, but not limited to, State Unemployment Compensation or Workers' Compensation. Vendor assumes the full responsibility for the acts and/or omissions of its employees or agents as they relate to the Products to be provided under this PA.

Vendor shall assume full responsibility for payment of all federal, state, and local taxes or contributions, including unemployment insurance, social security, and income taxes with respect to Vendor's employees.

24. FORCE MAJEURE

Neither party shall be deemed to be in violation of this PA if either is prevented from performing any of its obligations hereunder for any reason beyond its reasonable control, including but not limited to acts of God, natural disasters, earthquake, fire, flood, strikes, civil commotion, labor disputes, war, terrorism, infectious disease, and pandemics. If such an event continues for sixty (60) or more days, either party may terminate this PA by providing a written notification and shall not be liable to the other for failure to perform its obligation and any deposits or Vendor shall refund any pre-paid fees to Participant on a prorated basis.

25. COUNTERPARTS

This PA may be signed and delivered in two (2) counterparts, each of which, when so signed and delivered, shall be an original, but such counterparts together shall constitute the one instrument that is the PA, and the PA shall not be binding on any party until all parties have signed it.

26. AUTHORIZED SIGNATURES

The individual signing this PA warrants that he/she is authorized to do so. The parties understand and agree that a breach of this warranty shall constitute a breach of the PA and shall entitle the non-breaching party to all appropriate legal and equitable remedies against the breaching party.

IN WITNESS WHEREOF, the parties have executed this Purchase Agreement as of the Effective Date.

PARTICIPANT	**VENDOR**
______________________________	______________________________
By:	**By:**
Its:	**Its:**
_______________	_______________
Date	**Date**

Exhibit A

Order Information and Implementation Plan

Appendix B: Required Forms

All required forms must be submitted as part of the Vendor’s complete proposal on or before the Proposal Deadline specified in the calendar of events. Required Forms are listed below.

Proposal Submission Checklist
Master Agreement & Purchase Agreement Confirmation
Use of Form Agreements
Acknowledgment of Amendments to RFP
Vendor Representation and Certification
Noncollusion Declaration
Certification of Primary Participant Regarding Debarment, Suspension, and Other Responsibility Matters
Certification on Restrictions on Lobbying
Worker’s Compensation Certificate
Drug-Free workplace
Tobacco Use Policy
Criminal Records Check Certification by Vendor
Disclosure of Proposal
W-9
Insurance Requirements Acknowledgement
Minimum Price Guarantee Acknowledgment
Administrative Fee Acknowledgment
Rules Acknowledgement
Student Data Access
Manufacturer’s Letter(s) Authorizing Vendor to Sell
Authorized Resellers
Technical Specification and Requirements

PROPOSAL SUBMISSION CHECKLIST

- ❏ Proposal Submission Checklist (Appendix B)
- ❏ Master Agreement & Purchase Agreement Confirmation (Appendix B)
- ❏ Use of Form Agreements (Appendix B)
- ❏ Acknowledgment of Amendments to RFP (Appendix B)
- ❏ Vendor Representation and Certification (Appendix B)
- ❏ Noncollusion Declaration (Appendix B)
- ❏ Certification of Primary Participant Regarding Debarment, Suspension, and Other Responsibility Matters (Appendix B)
- ❏ Certification on Restrictions on Lobbying (Appendix B)
- ❏ Workers' Compensation Certificate (Appendix B)
- ❏ Drug Free Workplace Certification (Appendix B)
- ❏ Tobacco Use Policy (Appendix B)
- ❏ Criminal Records Check Certification by Vendor (Appendix B)
- ❏ Disclosure of Proposal (Appendix B)
- ❏ W-9 (Appendix B)
- ❏ Insurance Requirements Acknowledgement (Appendix B)
- ❏ Minimum Price Guarantee Acknowledgment (Appendix B)
- ❏ Administrative Fee Acknowledgment (Appendix B)
- ❏ Rules Acknowledgement (Appendix B)
- ❏ Student Data Access (Appendix B)
- ❏ Manufacturer's Letter(s) Authorizing Vendor to Sell
- ❏ Authorized Resellers
- ❏ Technical Specification and Requirements
- ❏ Federal Certifications (Appendix C)
- ❏ Pricing Form (Appendix D)
- ❏ Service Level and Maintenance Agreement (if applicable) (Appendix E)
- ❏ Sample Reports and Training Materials (Appendix E)
- ❏ Standard Student Data Privacy Agreement CA-NDPA (Appendix F)
- ❏ Proposal Form (Attachment 1)

Write out all answers using the Proposal Form in Attachment 1. Additional material may be submitted with the proposal as appendices. No brochures, marketing materials, or internal company documentation will be considered when scoring Proposals. Cross-references to the Proposal Form in additional materials will not be considered responsive. Any additional descriptive material that is used in support of any information in Vendor's proposal must be clearly identified.

MASTER AGREEMENT & PURCHASE AGREEMENT CONFIRMATION

Upon notification of selection and Board Approval by a Participant, the undersigned hereby promises and agrees to furnish all articles or services within the dates specified, in the manner and form and at the prices herein stated in strict accordance with the advertisement, specifications, proposals and general conditions all which are made a part of the Purchase Agreement.

Name under which business is conducted

Business Street Address City State Zip Code

Telephone Number:

IF SOLE OWNER, sign here:
I sign as sole owner of the business named above.

Signature Date

Name Title

IF PARTNERSHIP, sign here:
The undersigned certify that we are partners in the business named above and that we sign this purchase agreement with full authority so to do. (One (1) or more partners sign)

Signature Date

Name Title

Signature Date

Name Title

IF CORPORATION, sign here:

The undersigned certify that they sign this purchase agreement with full and proper authorization so to do.

Signature Date

Corporation Legal Name

Name Title

Incorporated under the laws of the State of

Use of Form Agreements

Vendors who agree to the provided template agreements may be given priority award, in the interest of providing agreements for use by Members. Requesting redlines will not affect a Vendor’s award status as long as JPA contracts take precedence and the parties can agree to terms, but may delay award and the availability of agreements for Member use. Awards shall be made contingent upon successful contract negotiations as determined by Ed Tech JPA’s sole discretion.

Vendors may include their licensing and/or other product-specific terms as an exhibit to the Purchase Agreement, with the Ed Tech JPA contracts taking precedence.

□ I hereby agree to using the provided **templates** for the Master Agreement, Purchase Agreement, and Standard Student Data Privacy Agreement (if applicable) and will not request redlines.

OR

□ I anticipate **requesting redlines** for the Master Agreement, Purchase Agreement, and Standard Student Data Privacy Agreement (if applicable).

Signature	Date
Vendor Legal Name	
Name	Title

ACKNOWLEDGEMENT OF AMENDMENTS TO RFP

VENDOR HEREBY ACKNOWLEDGES RECEIPT OF ANY AND ALL AMENDMENTS TO THE RFP.

If Vendor has no knowledge of any amendments to the RFP having been issued to, or received by, Vendor, please check the following box: □

Amendments

Amendment No	Date Published	Date Received

Signature	Date

Vendor Legal Name

Name	Title

VENDOR REPRESENTATION AND CERTIFICATION

The undersigned hereby acknowledges and affirms that:

- He/she is a duly authorized agent of the Vendor with the authority to submit a Proposal on behalf of the Vendor (corporate or other authorization confirmation may be requested prior to final contract execution).

- He/she has read the complete RFP documents and all amendments issued pursuant thereto.

- The Proposal complies with State conflict of interest laws. The Vendor certifies that no employee of its firm has discussed, or compared the Proposal with any other Vendor or District employee, and has not colluded with any other Vendor or District employee.

- If the Vendor's Proposal is accepted by Ed Tech JPA, the Vendor will enter into a Master Agreement with Participants to provide the Services, Systems and Equipment described by the Proposal on the terms mutually acceptable to Participants and the Vendor.

- Ed Tech JPA reserves the right to reject any or all proposals.

I hereby certify that I am submitting the attached Proposal on behalf of

I understand that, by virtue of executing and returning this required response form with the Proposal, I further certify, that the Vendor understands and does not dispute any of the contents of the proposal requirements (except as may be noted in the response).

Signature

Date

Vendor Legal Name

Name

Title

NOTE: If Joint Venture, each member of the joint venture must provide a completed certificate form.

NONCOLLUSION DECLARATION

TO BE EXECUTED BY VENDOR AND SUBMITTED WITH PROPOSAL
(Public Contract Code section 7106) The undersigned declares:
I am the

(title) of

(Vendor), the party making the foregoing proposal.
The proposal is not made in the interest of, or on behalf of, any undisclosed person, partnership, company, association, organization, or corporation. The proposal is genuine and not collusive or sham. The Vendor has not directly or indirectly induced or solicited any other vendor to put in a false or sham proposal. The Vendor has not directly or indirectly colluded, conspired, connived, or agreed with any vendor or anyone else to put in a sham proposal, or to refrain from submitting a proposal. The Vendor has not in any manner, directly or indirectly, sought by agreement, communication, or conference with anyone to fix the proposal price of the Vendor or any other vendor, or to fix any overhead, profit, or cost element of the proposal price, or of that of any other vendor. All statements contained in the proposal are true. The Vendor has not, directly or indirectly, submitted its proposal price or any breakdown thereof, or the contents thereof, or divulged information or data relative thereto, to any corporation, partnership, company, association, organization, proposal depository, or to any member or agent thereof, to effectuate a collusive or sham proposal, and has not paid, and will not pay, any person or entity for such purpose.
Any person executing this declaration on behalf of a Vendor that is a corporation, partnership, joint venture, limited liability company, limited liability partnership, or any other entity, hereby represents that he or she has full power to execute, and does execute, this declaration on behalf of the Vendor.

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct and that this declaration is executed as follows.

Signature

Date

Vendor Legal Name

Name

Title

City

State

CERTIFICATION OF PRIMARY PARTICIPANT REGARDING DEBARMENT, SUSPENSION, AND OTHER RESPONSIBILITY MATTERS

The

(Principal) of

(Vendor Name)

Certifies to the best of its knowledge and belief that it and its principals:

1. Are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions by any federal department or agency;
2. Have not within a three-year period preceding this proposal been convicted of or had a civil judgment rendered against them for commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (federal, state or local) transaction or contract under a public transaction; violation of federal or state antitrust statutes or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, or receiving stolen property;
3. Are not presently indicted for or otherwise criminally or civilly charged by a governmental entity (federal, state, or local), with commission of any of the offenses enumerated in paragraph (2) of this certification; and
4. Have not within a three-year period preceding this proposal had one (1) or more public transactions (federal, state or local) terminated for cause or default.

If unable to certify to any of the statements in this certification, the participant shall attach an expiration to this certification.

I HEREBY CERTIFY AND AFFIRM THE TRUTHFULNESS AND ACCURACY OF THE CONTENTS OF THE STATEMENTS SUBMITTED ON OR WITH THIS CERTIFICATION AND UNDERSTAND THAT THE PROVISIONS OF 31 U.S.C. SECTIONS 3801 ET SEQ. ARE APPLICABLE THERETO.

Signature Date

Vendor Legal Name

Name Title

CERTIFICATION OF RESTRICTIONS ON LOBBYING

I hereby certify on behalf of

(name of offeror) that

(Firm name) meets the following qualifications:

1. No Federal appropriated funds have been paid, by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer of employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of any Federal contract, the making of any Federal grant, the making of any Federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any Federal contract, grant, loan, or cooperative agreement.

2. If any funds, other than Federal appropriated funds, have been paid or will be paid to any person for influencing or attempting to Influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this Federal contract, grant, loan, or cooperative agreement, the undersigned shall complete and submit the attached, Standard Form-LLL, “Disclosure of Lobbying Activities”, in accordance with its instructions.

3. The undersigned shall require that the language of this certification be included in all subcontracts, and that all subcontractors shall certify and disclose accordingly.

This certification is a material representation of fact upon which reliance is placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering into this transaction imposed by section 1352, title 31, U.S. Code. Any person who fails to file the required certification shall be subject to civil penalty of not less than $10,000 and not more than $100,000 for each such failure.

Signature	Date

Vendor Legal Name

Name	Title

WORKERS' COMPENSATION CERTIFICATE

Labor Code Section 3700.

"Every employer except the state shall secure the payment of compensation in one or more of the following ways:

a. By being insured against liability to pay compensation in one or more insurers duly authorized to write compensation insurance in this state.

b. By securing from the Director of Industrial Relations a certificate of consent to self-insure either as an individual employer or as one employer in a group of employers, which may be given upon furnishing proof satisfactory to the Director of Industrial Relations of ability to self-insure and to pay any compensation that may become due to his or her employees.

c. For any county, city, city and county, municipal corporation, public DISTRICT, public agency or any political subdivision of the state, including each member of a pooling arrangement under a joint exercise of powers agreement (but not the state itself), by securing from the Director of Industrial Relations a certificate of consent to self-insure against workers' compensation claims, which certificate may be given upon furnishing proof satisfactory to the director of ability to administer workers' compensation claims properly, and to pay workers' compensation claims that may become due to its employees. On or before March 31, 1979, a political subdivision of the state which, on December 31, 1978, was uninsured for its liability to pay compensation, shall file a properly completed and executed application for a certificate of consent to self-insure against workers' compensation claims. The certificate shall be issued and be subject to the provisions of Section 3702."

I am aware of the provisions of Labor Code Section 3700 which require every employer to be insured against liability for workers' compensation or to undertake self-insurance in accordance with the provisions of that code, and I will comply with such provisions before commencing the performance of the work of this contract.

Signature Date

Vendor Legal Name

Name Title

(In accordance with Article 5 [commencing at Section 1860], Chapter 1, Part 7, Division 2 of the Labor Code, the above certificate must be signed and filed with the awarding body prior to performing any work under the contract.)

DRUG FREE WORKPLACE CERTIFICATION

This Drug-Free Workplace Certification is required pursuant to Government Code §8350, et seq., the Drug-Free Workplace Act of 1990. The Drug-Free Workplace Act of 1990 requires that every person or organization awarded a contract for the procurement of any property or services from any State agency must certify that it will provide a drug-free workplace by doing certain specified acts. In addition, the Act provides that each contract awarded by a State agency may be subject to suspension of payments or termination of the contract and the Vendor may be subject to debarment from future contacting, if the state agency determines that specified acts have occurred.

Pursuant to Government Code §8355, every person or organization awarded a contract from a State agency shall certify that it will provide a drug-free workplace by doing all of the following:

a. Publishing a statement notifying employees that the unlawful manufacture, distribution, dispensation, possession or use of a controlled substance is prohibited in the person's or organization's workplace and specifying actions which will be taken against employees for violations of the prohibition;

b. Establishing a drug-free awareness program to inform employees about all of the following:

i. The dangers of drug abuse in the workplace;

ii. The person's or organization's policy of maintaining a drug-free workplace;

iii. The availability of drug counseling, rehabilitation and employee-assistance programs;

iv. The penalties that may be imposed upon employees for drug abuse violations;

c. Requiring that each employee engaged in the performance of the contract be given a copy of the statement required by subdivision (a) and that, as a condition of employment on the contract, the employee agrees to abide by the terms of the statement.

I the undersigned, agree to fulfill the terms and requirements of Government Code §8355 listed above and will publish a statement notifying employees concerning (a) the prohibition of controlled substance at the workplace, (b) establishing a drug-free awareness program, and (c) requiring that each employee engaged in the performance of the contract be given a copy of statement required by §8355 (a) and requiring that the employee agree to abide by the terms of that statement.

I also understand that if the Participant determines that I have either (a) made false certification herein, or (b) violated this certification by failing to carry out the requirements of §8355, that the contract awarded herein is subject to suspension of payments, termination, or both. I further understand that, should I violate the terms of the Drug-Free Workplace Act of 1990, I may be subject to debarment in accordance with the requirements of §8350, et seq.

I acknowledge that I am aware of the provisions of Government Code §8350, et seq. and hereby certify that I will adhere to the requirements of the Drug-Free Workplace Act of 1990.

Signature	Date
Vendor Legal Name	
Name	Title

TOBACCO USE POLICY

In the interest of public health, Participant provides a tobacco-free environment. Smoking or the use of any tobacco products are prohibited in buildings and vehicles, and on any property owned, leased or contracted for, by the Participant. Failure to abide with this requirement could result in the termination of this contract.

I acknowledge that I am aware of Tobacco Use Policy and hereby certify that I and my employees will adhere to the requirements of the policy.

Signature	Date

Vendor Legal Name

Name	Title

NOTICE TO VENDORS REGARDING CRIMINAL RECORDS CHECK
(EDUCATION CODE §45125.1)

Education Code §45125.1 provides that if the employees of any entity that has a contract with a school DISTRICT may have any contact with pupils, those employees shall submit or have submitted their fingerprints in a manner authorized by the Department of Justice together with a fee determined by the Department of Justice to be sufficient to reimburse the Department for its costs incurred in processing the application.

The Department of Justice shall ascertain whether the individual whose fingerprints were submitted to it has been arrested or convicted of any crime insofar as that fact can be ascertained from information available to the Department. When the Department of Justice ascertains that an individual whose fingerprints were submitted to it has a pending criminal proceeding for a violent felony listed in Penal Code §1192.7(c) or has been convicted of such a felony, the Department shall notify the employer designated by the individual of the criminal information pertaining to the individual. The notification shall be delivered by telephone and shall be confirmed in writing and delivered to the employer by first-class mail.

The contract shall not permit an employee to come in contact with pupils until the Department of Justice has ascertained that the employee has not been convicted of a violent or serious felony. The Vendor shall certify in writing to the Board of Trustees of the school DISTRICT that none of its employees who may come in contact with pupils have been convicted of a violent or serious felony.

Penal Code §667.5(c) lists the following “violent” felonies: murder; voluntary manslaughter; mayhem; rape; sodomy by force; oral copulation by force; lewd acts on a child under the age of 14 years; any felony punishable by death or imprisonment in the state prison for life; any felony in which the defendant inflicts great bodily injury on another; any robbery perpetrated in an inhabited dwelling; arson; penetration of a person’s genital or anal openings by foreign or unknown objects against the victim’s will; attempted murder; explosion or attempt to explode or ignite a destructive device or explosive with the intent to commit murder; kidnapping; continuous sexual abuse of a child; and carjacking.

Penal Code §1192.7 lists the following : “serious” felonies: murder; voluntary manslaughter; mayhem; rape; sodomy by force; oral copulation by force; a lewd or lascivious act on a child under the age of 14 years; any felony punishable by death or imprisonment in the state prison for life; any felony in which the defendant personally inflicts great bodily injury on another, or in which the defendant personally uses a firearm; attempted murder; assault with intent to commit rape or robbery; assault with a deadly weapon on a peace officer; assault by a life prisoner on a non-inmate; assault with a deadly weapon by an inmate; arson; exploding a destructive device with intent to injure or to murder, or explosion causing great bodily injury or mayhem; burglary of an inhabited dwelling; robbery or bank robbery; kidnapping; holding of a hostage by a person confined in a state prison; attempt to commit a felony punishable by death or imprisonment in the state prison for life; any felony in which the defendant personally uses a dangerous or deadly weapon; selling or furnishing specified controlled substances to a minor; penetration of genital or anal openings by foreign objects against the victim’s will; grand theft involving a firearm; carjacking; and a conspiracy to commit specified controlled substances offenses.

CRIMINAL RECORDS CHECK CERTIFICATION BY VENDOR

(AB 1610, 1612 and 2102)

To the Board of Trustees of Participant:

I,

(name)

certify that:

(Name of Vendor)

1. has carefully read and understands the Notice to Vendors Regarding Criminal Record Checks (Education Code §45125.1) required by the passage of AB 1610, 1612 and 2102.

2. Due to the nature of the work it will be performing for the Participant,

(Name of Vendor)

employees may have contact with students of the DISTRICT.

3. None of the employees who will be performing the work have been convicted of a violent or serious felony as defined in the Notice and in Penal Code §1192.7 and this determination was made by a fingerprint check through the Department of Justice.

I declare under penalty of perjury that the foregoing is true and correct.

Signature Date

Vendor Legal Name

Name Title

City State

DISCLOSURE OF PROPOSAL

⬜ I hereby agree to the posting of this **full Proposal** and supporting documents on a password protected website available only to active Ed Tech JPA Members.

OR

⬜ I agree to the posting of a **redacted Proposal** and supporting documents on a password protected website available only to active Ed Tech JPA Members.

Signature	Date

Vendor Legal Name

Name	Title

W-9

Current Version Available at: http://www.irs.gov/pub/irs-pdf/fw9.pdf

Please be sure to enter Vendor’s full legal name. This is the name that will be used for awarded vendors.

Insurance Requirements Acknowledgement

These are the Insurance Requirements for Vendors providing services or supplies to Ed Tech JPA, and its Founding Members and Associate Members. By submitting a proposal, you verify that you comply with and agree to be bound by these requirements. If any additional Contract documents are executed, the actual Insurance Requirements may include additional provisions as deemed appropriate by Ed Tech JPA and the Participant. All insurers must be duly licensed and admitted by the State of California.

Mandatory Requirements (unless Participant reduces or excludes coverage requirements)

1. Commercial General Liability insurance for bodily injury and property damage, including accidental death in the combined single limit of not less than $1,000,000 per occurrence ($2,000,000 aggregate) and $3,000,000 Excess/Umbrella Liability.

Minimum Limits (If required by Participant)

1. Workers' Compensation and Employer's Liability insurance in the amount of not less than $1,000,000 per occurrence.

2. Professional Liability insurance in an amount of not less than $1,000,000 per occurrence ($2,000,000 aggregate). If Professional Liability policy is made on a claims-made basis, the vendor/consultant must purchase and maintain an extending reporting period (tail coverage) for one year.

Any insurance proceeds in excess of the specified limits and coverage required, which are applicable to a given loss, shall be available to Ed Tech JPA or Participant, as applicable. No representation is made that the minimum Insurance requirements of this agreement are sufficient to cover the indemnity or other obligations of the Vendor under this RFP, Master Agreement and Purchase Agreements with Associate Members.

Optional Insurance

Cyber Risk insurance to cover both tangible and intangible property risk of the system and data, as well as third party liability for breaches of security is encouraged, but not required by EdTech JPA. Desired coverage includes: i. Security and privacy liability, including privacy breach response costs, regulatory fines and penalties; ii. Media liability, including infringement of copyright, trademark and trade dress (intellectual property by appearance of product, design, or packaging); iii. Cyber extortion; and iv. Privacy. Suggested limits of not less than $2,000,000 per occurrence, or sufficiently broad to respond to the duties and obligations as is undertaken by the Vendor in this RFP, Master Agreement and Purchase Agreements with Associate Members. The Policy should include, or be endorsed to include, property damage liability coverage for damage to, alteration of, loss of, or destruction of electronic data and/or information "property" of the Agency in the care, custody, or control of the Vendor.

Additional Insured Endorsement Language

"[Participant Name], its Board of Trustees, officers, agents, employees, and volunteers are named as additionally insured on this policy pursuant to written contract, agreement, or memorandum of understanding. Such insurance as is afforded by this policy shall be primary, and any insurance carried by District shall be excess and noncontributory."

Additional Insured Endorsements are required to accompany Certificates of Insurance. Certificate of Insurance shall provide thirty (30) days prior written notice of cancellation.

Additional Required Documents

Certificates of Insurance must be accompanied by a list of all excluded coverages under the general liability and excess/umbrella liability policies. The exclusion policy document section must be provided to Participants. The general liability and excess/umbrella liability documents must list the corresponding policy numbers referenced on the Certificate of Insurance.

Individual Associate Member Requirements

Individual Associate Members may have different/additional requirements than the minimum insurance requirements specified herein. Vendor agrees to maintain insurance that meets the requirements of individual Associate Members.

I hereby agree to the insurance requirements specified herein.

Signature

Date

Vendor Legal Name

Name

Title

Minimum Price Guarantee Acknowledgment

To prevent underpricing and protect seller Margin, Vendor’s pricing shall be subject to a Minimum Price Guarantee (MPG), whereby, Vendor shall agree not to sell directly, or through a reseller, to Ed Tech JPA’s Eligible Entities located in California (regardless of whether the Eligible Entity is an Associate Member of the Ed Tech JPA), including all California public school districts, county offices of education, and community college districts, and any other public agency in California whose procurement rules, whether internal rules or rules enacted pursuant to statute, allow them to purchase goods or services through a procurement vehicle such as Ed Tech JPA, the Products(s) subject to the Master Agreement at a price lower than the price offered pursuant to the RFP and the Master Agreement.

During the period of delivery under a contract resulting from this RFP, if the price of an item decreases, Ed Tech JPA Participants shall receive a corresponding decrease in prices on the balance of the deliveries for as long as the lower prices are in effect. Vendor agrees to amend the Master Agreement to reflect the decreased pricing. At no time shall the prices charged to Ed Tech JPA Participants exceed the prices under which the RFP was awarded. Ed Tech JPA Participants shall be given the benefit of any lower prices which may, for comparable quality and delivery, be given by the Vendor to any other school district or any other state, county, municipal or local government agency in a California County for the product(s) listed in the RFP.

I hereby agree to the Minimum Price Guarantee specified herein.

Signature	Date

Vendor Legal Name

Name	Title

Administrative Fee Acknowledgment

Vendor agrees to pay Ed Tech JPA an administrative fee (the “Admin Fee”) calculated as four percent (4%) of the invoiced amount of any Participant agreement with Vendor based on an award under the RFP and all revenue derived directly from any PA, including any additional services, and agreement extensions or renewals. Individual Transactions that meet a certain dollar amount will receive a discount and pay Admin Fees as listed on the JPA website at:

https://edtechjpa.org/administrative-fee

Computations of the Admin Fee shall exclude state, local, or federal taxes levied on invoiced amounts. The Admin Fee must be included when determining the pricing offered. The Admin Fee is not negotiable and shall not be added as a separate line item on an invoice. The Admin Fee is not refundable to Participants or Vendors under any circumstances.

I hereby agree to the Administrative Fee specified herein.

Signature	Date

Vendor Legal Name

Name	Title

Rules Acknowledgement

I hereby agree to the Rules specified in Section 6.0 of this RFP.

Signature Date

Vendor Legal Name

Name Title

Student Data Access

□ I hereby certify that the proposed Solution does **NOT** have access to student data.

OR

□ The proposed Solution **may have access** to student data and a Standard Student Data Privacy Agreement may be required.

Signature Date

Vendor Legal Name

Name Title

MANUFACTURER’S LETTER(S) AUTHORIZING BIDDER TO SELL

If Vendor is a reseller, please provide letters from the manufacturer(s) showing the Vendor is an approved reseller.

AUTHORIZED RESELLERS

If Vendor is a Manufacturer, please provide the legal name of all authorized resellers that Vendor authorizes to sell the Solution under this RFP:

Reseller Legal Name	Contact Name	Contact Email	Contact Phone Number

Signature	Date

Vendor Legal Name

Name	Title

TECHNICAL SPECIFICATIONS AND REQUIREMENTS:

This form is required only for Vendors proposing physical goods (equipment and supplies) in response to this RFP. Vendors proposing exclusively professional services and/or software as a service are not required to submit this form.

As technology advances, it is understood that improved or enhanced equipment may supersede existing equipment in both price and performance and yet be essentially similar. This request for proposals seeks to address the rapid advances in technology by allowing functionally similar or identical products that may be introduced in the future, during the term of the awarded Agreement(s), to be included under the general umbrella of compatible product lines and are thus specifically included in these RFP Documents.

As new models are introduced in the future, this bid and the resulting Agreement(s) will allow purchases of those models. The price will be determined by the awarded Vendor(s) subtracting the same discount margin percentage to these models, as calculated on current models. Vendor may be required to produce list/price or manufacturer costs.

All sales of equipment and supplies must be from authorized dealers only, with proof provided by manufacturer.

Participants may purchase (at their discretion) additional units throughout the life of the Agreement at the prices listed in awarded Vendors' Pricing Sheet, allowing only price increases reflecting original manufacturer's cost increases to the awarded Vendor. Documentation may be required to prove price increase from the manufacturer to the awarded Vendor.

Purchases by Participant(s) to the successful Vendor for awarded products shall be in the form of a Purchase Order.

I understand and agree to all conditions listed above.

Signature	Date

Vendor Legal Name

Name	Title

Appendix C: Federal Certifications

Education Department of General Administration Regulation (EDGAR) Federal Funding Contract Compliance Form

The following provisions are not required for award but may be required by Participants and apply when federal funds are expended by Participants for any contract resulting from this procurement process. Participants are the sub grantee or sub recipient by definition.
In addition to other provisions required by the federal agency or non-Federal entity, all contracts made by the non-Federal entity under the Federal award must contain provisions covering the following, as applicable.

Breach of Contract by Either Parties

Contracts for more than the simplified acquisition threshold currently set at $250,000 which is the inflation adjusted amount determined by the Civilian Agency Acquisition Council and the Defense Acquisition Regulations Council (Councils) as authorized by 41 U.S.C. 1908, must address administrative, contractual, or legal remedies in instances where contractors violate or breach contract terms, and provide such sanctions and penalties as appropriate.

Pursuant to the Federal Rules above, when federal funds are expended by Participants District, the Participant reserves all rights and privileges under the applicable laws and regulations with respect to this procurement in the event of breach of contract by either party.

I hereby agree to the Breach of Contract by Either Parties

Initials of Authorized Representative of Vendor	Name

Termination For Cause or For Convenience

Termination for cause or for convenience by the grantee or sub grantee including the manner by which it will be affected and the basis for settlement. (All contracts in excess of $10,000)

Pursuant to the Federal Rules above, when federal funds are expended by Participants, Participants reserve all rights to immediately terminate any agreement in excess of $10,000 resulting from this procurement process in the event of a breach or default of the agreement by Vendor, in the event Vendor fails to: (1) meet schedules, deadlines, and/or delivery dates within the time specified in the procurement solicitation, contract, and/or a purchase order; (2) make any payments owed; or (3) otherwise perform in accordance with the contract and/or the procurement solicitation. Participants also reserve the right to terminate the contract immediately, with written notice to Vendor, for convenience, if Participant believes, in its sole discretion that it is in the best interest of Participant to do so. The Vendor will be compensated for work performed and accepted and goods accepted by Participant as of the termination date if the contract is terminated for convenience of Participant. Any award under this procurement process is not exclusive and Participants reserve the right to purchase goods and services from other vendors when it is in the best interest Participants.

I hereby agree to the Termination For Cause or For Convenience

Initials of Authorized Representative of Vendor	Name

Rights to Inventions Made Under a Contract Agreement

Rights to Inventions Made Under a Contract Agreement. If the Federal award meets the definition of “funding agreement” under 37 CFR §401.2(a) and the recipient or sub recipient wishes to enter into a contract with a small business firm or nonprofit organization regarding the substitution of parties, assignment or performance of experimental, developmental, or research work under that “funding agreement, “; the recipient or sub recipient must comply with the requirements of 37 CFR Part 401, “Rights to Inventions Made by Nonprofit Organizations and Small Business Firms Under Government Grants, Contracts and Cooperative Agreements,” and any implementing regulations issued by the awarding agency.

Pursuant to the Federal Rules above, when federal funds are expended by Participants, the Vendor certifies that during the term of an award for all contracts by Participants resulting from this procurement process, the Vendor agrees to comply with all applicable requirements as referenced in Federal Rule (C) above.

I hereby agree to the Rights to Inventions Made Under a Contract Agreement

Initials of Authorized Representative of Vendor	Name

Clean Air Act (42 U.S.C.7401-7671q.)
Clean Air Act (42 U.S.C. 7401-7671q.) and the Federal Water Pollution Control Act (33 U.S.C. 1251-1387), as amended – Contracts and sub grants of amounts in excess of $250,000 must contain a provision that requires the non-Federal award to agree to comply with all applicable standards, orders or regulations issued pursuant to the Clean Air Act (42 U.S.C. 7401-7671q) and the Federal Water Pollution Control Act as amended (33 U.S.C. 1251-1387). Violations must be reported to the Federal awarding agency and the Regional Office of the Environmental Protection Agency (EPA).

Pursuant to the Federal Rules above, when federal funds are expended by Participants, the Vendor certifies that during the term of an award for all contracts by Participants resulting from this procurement process, the Vendor agrees to comply with all applicable requirements as referenced in the Federal Rules above.

I hereby agree to the Clean Air Act (42 U.S.C. 7401-7671q.)

Initials of Authorized Representative of Vendor	Name

Debarment and Suspension
Debarment and Suspension (Executive Orders 12549 and 12689) – A contract award (see 2 CFR 180.220) must not be made to parties listed on the government wide exclusions in the system for Award Management (SAM), in accordance with the OMB guidelines at 2 CFR 180 that implement Executive Orders 12549 (3 CFR part 1986 Comp., p. 189) and 12689 (3 CFR part 1989 Comp., p.235), “Debarment and Suspension”. SAM exclusions contain the names of parties debarred, suspended or otherwise excluded by agencies, as well as parties declared ineligible under statutory or regulatory authority other than Executive Order 12549.

Pursuant to the Federal Rules above, when federal funds are expended by Participants, the Vendor certifies that during the term of an award for all contracts by Participants resulting from this procurement process, the Vendor certifies that neither it nor its principals is presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation by any federal department or agency.

I hereby agree to the Debarment and Suspension

Initials of Authorized Representative of Vendor	Name

Byrd Anti-Lobbying Amendment (31 U.S.C. 1352)
(Byrd Anti-Lobbying Amendment (31 U.S.C. 1352) – Contractors that apply or bid for an award exceeding $100,000 must file the required certification. Each tier certified to the tier above that it will not and has not used Federal appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of any agency, a

member of Congress, officer or employee of Congress, or an employee of a member of Congress in connection with obtaining any Federal contract, grant or any other award covered by 31 U.S.C. 1352. Each tier must also disclose any lobbying with non-Federal funds that take place in connection with obtaining any Federal award. Such disclosures are forwarded from tier to tier up to the non-Federal award.

Pursuant to the Federal Rules above, when federal funds are expended by Participants, the Vendor certifies that during the term and after the awarded term of an award for all contracts by Participants resulting from this procurement process, the Vendor certifies that it is in compliance with all applicable provisions of the Byrd Anti-Lobbying Amendment (31 U.S.C. 1352). The undersigned further certifies that

a.) No Federal appropriated funds have been paid or will be paid for on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of congress, or an employee of a Member of Congress in connection with the awarding of a Federal contract, the making of a Federal grant, the making of a Federal loan, the entering into a cooperative agreement, and the extension, continuation, renewal, amendment, or modification of a Federal contract, grant, loan, or cooperative agreement.

b.) If any funds other than Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of congress, or an employee of a Member of Congress in connection with this Federal grant or cooperative agreement, the undersigned shall complete and submit Stand Form-LLL, “Disclosure Form to Report Lobbying”, in accordance with its instructions

c.) The undersigned shall require that the language of this certification be included in the award documents for all covered sub-awards exceeding $100,000 in Federal funds to all appropriate tiers and that all sub recipients shall certify and disclose accordingly.

I hereby agree to the Byrd Anti-Lobbying Amendment (31 U.S.C. 1352)

Initials of Authorized Representative of Vendor	Name

Record Retention Requirements for Contracts Paid For With Federal Funds - 2 CFR § 200.333

When federal funds are expended by Participants for any contract resulting from this procurement process, the Vendor certifies that it will comply with the record retention requirements detailed in 2 CFR § 200.333. The Vendor further certifies that Vendor will retain all records as required by 2 CFR § 200.333 for a period of three years after grantees or sub grantees submit final expenditure reports or quarterly or annual financial reports, as applicable, and all other pending matters are closed.

I hereby agree to the Record Retention Requirements for Contracts Paid For With Federal Funds - 2 CFR § 200.333

Initials of Authorized Representative of Vendor	Name

Certification of Compliance With the Energy Policy and Conservation Act

When federal funds are expended by Participants for any contract resulting from this procurement process, the Vendor certifies that it will be in compliance with mandatory standards and policies relating to energy efficiency which are contained in the state energy conservation plan issued in compliance with the Energy Policy and Conservation Act (42 U.S.C. 6321, et seq.; 49 C.F.R. Part 18; Pub. L. 94-163, 89 Stat. 871).

I hereby agree to the Certification of Compliance With the Energy Policy and Conservation Act

Initials of Authorized Representative of Vendor Name

Certification of Compliance with Buy America Provisions

Vendor certifies that Vendor is in compliance with all applicable provisions of the Buy America Act. Purchases made in accordance with the Buy America Act must still follow the applicable procurement rules calling for free and open competition.

I hereby agree to the Certification of Compliance with Buy America Provisions

Initials of Authorized Representative of Vendor Name

Certification of Non-Collusion Statement

Vendor certifies under penalty of perjury that its response to this procurement solicitation is in all respects bona fide, fair, and made without collusion or fraud with any person, joint venture, partnership, corporation or other business or legal entity.

I hereby agree to the Certification of Non-Collusion Statement

Initials of Authorized Representative of Vendor Name

Vendor agrees to comply with all federal, state, and local laws, rules, regulations and ordinances, as applicable. It is further acknowledged that Vendor certifies compliance with all provisions, laws, acts, regulations, etc. as specifically noted above

Vendor Legal Name

Vendor Address

City State Zip

Phone Number Fax Number

Email Address

Name Title

Signature Date

Appendix D: Pricing Form

Detail all costs associated with the proposed Solution, including, but not limited to, equipment and/or product purchase costs, delivery, implementation, installation, configuration, software licensing, maintenance, ongoing support, repairs, parts, recommended professional services, taxes and surcharges, and costs of optional services and products. Describe any assumptions made impacting the cost proposal, and any limitations (e.g., professional service hours, minimum quantities/licenses) that apply to the listed costs. Costs not identified by the Vendor shall be borne by the Vendor and will not alter the requirements identified in this solicitation.

Please submit PDF and Excel versions of your pricing form with your proposal.

Ed Tech JPA Security and IT Admin RFP - Pricing Form

Please complete the pricing form below. Refer to the second tab of this spreadsheet for additional definitions and instructions. Samples are provided in the sheet to illustrate how Vendors may approach pricing a variety of offerings, incluidng equipment, software, and services. Additionally, Vendors may choose to offer standard discount percentages (rather than fixed prices) for purchases.

Line Number	Vendor Reference/Model Number (Optional)	Proposed Solution	Solution Type	Pricing Model	JPA Member Unit Price or Discount Amount/Percentage	Unit Definition/Pricing Basis	Purchase Requirements (volume)	Purchase Type (one-time, annual license)	Comments/Description
Use this number where requested in the requirements section.	Unique model number or item number for Vendor reference.	Title or short description of the proposed item(s). Each item or bundle of items should be placed on a separate line.	Type of item(s) proposed.	Indicate whether proposed items are offered at a set price or a set discount level from MSRP or equivalent.	List the unit price of the item or standard discount that will be applied. **Unit Price:** For equipment, list the cost of a single unit. For software, list the cost per license. Do NOT include Sales Tax. **Discount Amount/Percentage:** List the percentage or amount discount off of MSRP or Vendor's published/standard prices.	Describe what constitutes a unit. For example, if software is licensed based on student enrollment, Vendor might state (per student, based on total enrollment).	Indicate any threshold requirements (e.g., pricing tiers or minimum purchase amount) customers must meet to qualify for the pricing described in this line item (e.g., >30,000 studnets, minimum 20 units, purchases greater than $100,000).	Indicate whether the purchase is a one-time cost (implementation services, equipment purchase) or an annual cost (software subscription, maintenance).	
S1	*12345*	*Sample Vendor-Hosted Software Platform (Tier 1)*	*Software (Subsc…*	*Set Price*	*$2.00*	*Per Student (Total Enrollment)*	*>30,000 Students*	*Recurring (Annu…*	
S2	*54321*	*Sample Vendor-Hosted Software Platform (Tier 2)*	*Software (Subsc…*	*Set Price*	*$2.50*	*Per Student (Total Enrollment)*	*10,000 - 29,999 Students*	*Recurring (Annu…*	
S3	*25648-34645*	*Sample Catalog Discount - Security Cameras*	*Brand/Catalog D…*	*Standard Disc…*	*20%*	*Discount off MSRP*	*n/a*	*One-Time*	
S4	*84569*	*Sample Next Gen Firewall and Filter (Hardware)*	*Equipment/Supp…*	*Set Price*	*$150,000.00*	*Per Unit*	*n/a*	*One-Time*	
S5	*91548*	*Sample Next Gen Firewall and Filter (Maintenance)*	*Software (Subsc…*	*Set Price*	*$25,000.00*	*Per Unit*	*n/a*	*Recurring (Annu…*	
S6	*n/a*	*Sample Professional Services - Incident Response/Investigation*	*Professsional Se…*	*Set Price*	*$250.00*	*Per Hour*	*min 10/hrs per incident*	*One-Time*	
1									
2									
3									
4									
5									
6									
7									
8									
9									
10									

Line Number	Requirements Section(s) (Related to Proposed Item)																					
	3.1	3.2	3.3	3.4	3.5	3.6	3.7	3.8	3.9	3.10	3.11	3.12	3.13	3.14	3.15	3.16	3.17	3.18	3.19	3.20	4.1	4.2	4.3
	Inventory (Hardware)	Inventory (Software)	Data Protection	Secure Config.	Account Mgt	Access Control	Vulnerability Mgt	Audt Log Mgt	Email/Browser Sec	Malware Defense	Data Recovery	Net. Infrastructure Mgt	Net. Monitoring	Security Training	Svc. Provider Mgt	Application Sec.	Incident Response	Pen Testing	Sec. Services	Campus/Facility Safey	Help Desk	Project Mgt	Classroom Mgt
S1	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	☑	□	□	☑
S2	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	☑	□	□	☑
S3	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	☑	☑	□	□	□
S4	□	□	□	□	□	☑	☑	□	☑	☑	□	☑	☑	□	□	□	□	□	□	□	□	□	□
S5	□	□	□	□	□	☑	☑	□	☑	☑	□	☑	☑	□	□	□	□	□	□	□	□	□	□
S6	□	□	□	□	□	□	□	☑	□	□	□	□	□	☑	□	□	☑	□	☑	□	□	□	□
1	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
2	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
3	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
4	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
5	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
6	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
7	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
8	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
9	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
10	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

Appendix E: Supplementary Materials

Service Level and Maintenance Agreement (if applicable)
Sample Reports and Training Materials
Additional Resources that Support the Proposal

Appendix F: Standard Student Data Privacy Agreement (CA-NDPA Standard)

Please complete and sign the CA-NDPA, including Exhibit E, if your Solution may have access to student data, so Ed Tech JPA Members can agree to the same terms.

Ed Tech JPA

and

Provider

DATE

This Student Data Privacy Agreement ("DPA") is entered into on DATE (the "Effective Date") and is entered into by and between: Education Technology Joint Powers Authority (the **"Local Education Agency"** or **"LEA")**, located at 5050 Barranca Parkway, Irvine, CA 92604, and VENDOR (the **"Provider")**, located at ADDRESS

WHEREAS, the Provider is providing educational or digital services to LEA.

WHEREAS, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act **("FERPA")** at 20 U.S.C. § 1232g (34 CFR Part 99); the Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations and

WHEREAS, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.

NOW THEREFORE, for good and valuable consideration, LEA and Provider agree as follows:

1. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the Standard Clauses hereto.
2. **Special Provisions. *Check if Required***

__X__________ If checked, the Supplemental State Terms and attached hereto as **Exhibit "G"** are hereby incorporated by reference into this DPA in their entirety.

__X______If Checked, the Provider, has signed **Exhibit "E"** to the Standard Clauses, otherwise known as General Offer of Privacy Terms.

3. In the event of a conflict between the SDPC Standard Clauses, the State or Special Provisions will control. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider Terms of Service or Privacy Policy the terms of this DPA shall control.

4. This DPA shall stay in effect for five (5) years. Exhibit E will expire five (5) years from the date the original DPA was signed.

5. The services to be provided by Provider to LEA pursuant to this DPA are detailed in **Exhibit "A"** (the **"Services").**

6. **Notices**. All notices or other communication required or permitted to be given hereunder may be given via e-mail transmission, or first-class mail, sent to the designated representatives below.

The designated representative for the LEA for this DPA is:
Name: Michelle Bennett______________________________Title:Procurement Specialist

Address: 5050 Barranca Parkway, Irvine, CA 92604

Phone: 949-936-5022______________________________Email: edtechjpa@iusd.org

The designated representative for the Provider for this DPA is:

Name:____Title:________________________________

Address: ____

Phone:____Email: _______________________

IN WITNESS WHEREOF, LEA and Provider execute this DPA as of the Effective Date.

LEA: Education Technology Joint Powers Authority

By:____Date:_________________________

Printed Name:__ Brianne Ford ________________________Title/Position:_ President

PROVIDER: NAME

By:____Date:_________________________________

Printed Name:______________________________________Title/Position:__________________________

STANDARD CLAUSES

Version 3.0

ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of DPA.** The purpose of this DPA is to describe the duties and responsibilities to protect Student Data including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. In performing these services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA, with respect to its use of Student Data

2. **Student Data to Be Provided.** In order to perform the Services described above, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as **Exhibit "B"**.

3. **DPA Definitions.** The definition of terms used in this DPA is found in **Exhibit "C"**. In the event of a conflict, definitions used in this DPA shall prevail over terms used in any other writing, including, but not limited to the Service Agreement, Terms of Service, Privacy Policies etc.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA.** All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement, shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEA as it pertains to the use of Student Data, notwithstanding the above.

2. **Parent Access.** To the extent required by law the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner (and no later than forty-five (45) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LEA's request for Student Data in a student's records held by the Provider to view or correct as necessary. In the event that a parent of a student or other individual

contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.

3. **Separate Account.** If Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Student Generated Content to a separate account created by the student.

4. **Law Enforcement Requests.** Should law enforcement or other government entities {"Requesting Party(ies)") contact Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request.

5. **Subprocessors.** Provider shall enter into written agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Provide Data in Compliance with Applicable Laws.** LEA shall provide Student Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.

2. **Annual Notification of Rights.** If the LEA has a policy of disclosing Education Records and/or Student Data under FERPA {34 CFR § 99.31{a){l)), LEA shall include a specification of criteria for determining who constitutes a School Official and what constitutes a legitimate educational interest in its annual notification of rights.

3. **Reasonable Precautions.** LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted Student Data.

4. **Unauthorized Access Notification.** LEA shall notify Provider promptly of any known unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance.** The Provider shall comply with all applicable federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from time to time.

2. **Authorized Use.** The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in Exhibit A and/or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA.

3. **Provider Employee Obligation.** Provider shall require all of Provider's employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the Student Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each

employee or agent with access to Student Data pursuant to the Service Agreement.

4. **No Disclosure.** Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non-public information and/or Personally Identifiable Information contained in the Student Data other than as directed or permitted in writing by the LEA or this DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to Subprocessors performing services on behalf of the Provider pursuant to this DPA. Provider will not Sell Student Data to any third party.

5. **De-Identified Data:** Provider agrees not to attempt to re-identify de-identified Student Data. De-Identified Data may be used by the Provider for those purposes allowed under FERPA and the following purposes:
(1) assisting the LEA or other governmental agencies in conducting research and other studies; and (2) research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Except for Subprocessors, Provider agrees not to transfer de identified Student Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to the LEA who has provided prior written consent for such transfer. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which de-identified data is presented.

6. **Disposition of Data.** Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data after providing the LEA with reasonable prior notice. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to Article II section 3. The LEA may employ a "Directive for Disposition of Data" form, a copy of which is attached hereto as **Exhibit "D".** If the LEA and Provider employ Exhibit "D," no further written request or notice is required on the part of either party prior to the disposition of Student Data described in Exhibit "D”.

7. **Advertising Limitations.** Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits.

ARTICLE V: DATA PROVISIONS

1. **Data Storage.** Where required by applicable law, Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.

2. **Audits.** No more than once a year, or following unauthorized access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA The Provider will cooperate reasonably with the LEA and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the

Provider, LEA and delivery of Services to the LEA. Failure to reasonably cooperate shall be deemed a material breach of the DPA.

3. **Data Security.** The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. The Provider shall implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth in **Exhibit "F".** Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment to **Exhibit "F".** Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit "F".** Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.

4. **Data Breach**. In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider the Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:

(1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:

i. The name and contact information of the reporting LEA subject to this section.

ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.

iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and

v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

(2) Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.

(3) Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including Personally Identifiable Information and agrees to provide LEA, upon request, with a summary of said written incident response plan.

(4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians.

(5) In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

ARTICLE VI: GENERAL OFFER OF TERMS

Provider may, by signing the attached form of "General Offer of Privacy Terms" (General Offer, attached hereto as **Exhibit "E"**. be bound by the terms of **Exhibit "E"** to any other LEA who signs the acceptance on said Exhibit. The form is limited by the terms and conditions described therein.

ARTICLE VII: MISCELLANEOUS

1. **Termination.** In the event that either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated. Either party may terminate this DPA and any service agreement or contract if the other party breaches any terms of this DPA.

2. **Effect of Termination Survival.** If the Service Agreement is terminated, the Provider shall destroy all of LEA's Student Data pursuant to Article IV, section 6.

3. **Priority of Agreements.** This DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between Exhibit H, the SDPC Standard Clauses, and/or the Supplemental State Terms, Exhibit H will control, followed by the Supplemental State Terms. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

4. **Entire Agreement.** This DPA and the Service Agreement constitute the entire agreement of the Parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the Parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both Parties. Neither failure nor delay on the part of any Party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.

5. **Severability.** Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the Parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.

6. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE LEA, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY OF THE LEA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.

7. **Successors Bound.** This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DPA, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the DPA and any obligations with respect to Student Data within the Service Agreement. The LEA has the authority to terminate the DPA if it disapproves of the successor to whom the Provider is

selling, merging, or otherwise disposing of its business.

8. **Authority.** Each party represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof.

9. **Waiver.** No delay or omission by either party to exercise any right hereunder shall be construed as a waiver of any such right and both parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

EXHIBIT "A"

DESCRIPTION OF SERVICES

[INSERT DETAILED DESCRIPTION OF PRODUCTS AND SERVICES HERE.
IF MORE THAN ONE PRODUCT (RESOURCE) OR SERVICE IS INCLUDED, LIST EACH PRODUCT (RESOURCE) HERE]

EXHIBIT "B"

SCHEDULE OF DATA

Category of Data	Elements	Check if Used by Your System
Application Technology Meta Data	IP Addresses of users, Use of cookies, etc.	
	Other application technology meta data- Please specify:	
Application Use Statistics	Meta data on user interaction with application	
Assessment	Standardized test scores	
	Observation data	
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications captured (emails, blog entries)	
Conduct	Conduct or behavioral data	

Demographics	Date of Birth	
	Place of Birth	
	Gender	
	Ethnicity or race	
	Language information (native, or primary language spoken by student)	
	Other demographic information-Please specify:	
Enrollment	Student school enrollment	
	Student grade level	
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information-Please specify:	

Parent/Guardian Contact Information	Address	
	Email	
	Phone	

Category of Data	Elements	Check if Used by Your System
Parent/Guardian ID	Parent ID number (created to link parents to students)	
Parent / Guardian Name	First and/or Last	
Schedule	Student scheduled courses	
	Teacher names	
Special Indicator	English language learner information	
	Low income status	
	Medical alerts/ health data	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information-Please specify:	
Student Contact Information	Address	

	Email	
	Phone	
Student Identifiers	Local (School district) ID number	
	State ID number	
	Provider/App assigned student ID number	
	Student app username	
	Student app passwords	
Student Name	First and/or Last	
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	
Student work	Student generated content; writing, pictures, etc.	
	Other student work data -Please specify:	
Transcript	Student course grades	

	Student course data	
	Student course grades/ performance scores	

Category of Data	Elements	Check if Used By Your System
	Other transcript data - Please specify:	
Transportation	Student bus assignment	
	Student pick up and/or drop off location	
	Student bus card ID number	
	Other transportation data - Please specify:	
Other	Please list each additional data element used, stored, or collected by your application:	
None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable .	

EXHIBIT *"C:"'* DEFINITIONS

De-Identified Data and De-Identification: Records and information are considered to be de-identified when all Personally Identifiable Information has been removed or obscured, such that the remaining information does not reasonably identify a specific individual, including, but not limited to, any information that, alone or in combination is linkable to a specific student and provided that the educational agency, or other party, has made a reasonable determination that a student's identity is not personally identifiable, taking into account reasonable available information.

Educational Records: Educational Records are records, files, documents, and other materials directly related to a student and maintained by the school or local education agency, or by a person acting for such school or local education agency, including but not limited to, records encompassing all the material kept in the student's cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs.

Metadata: means information that provides meaning and context to other data being collected; including, but not limited to: date and time records and purpose of creation Metadata that have been stripped of all direct and indirect identifiers are not considered Personally Identifiable Information.

Operator: means the operator of an internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used for K-12 school purposes. Any entity that operates an internet website, online service, online application, or mobile application that has entered into a signed, written agreement with an LEA to provide a service to that LEA shall be considered an "operator" for the purposes of this section.

Originating LEA: A local education agency who originally executes the DPA in its entirety with the Provider.

Provider: For purposes of the DPA, the term "Provider" means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Student Data. Within the DPA the term "Provider" includes the term "Third Party" and the term "Operator" as used in applicable state statutes.

Student Generated Content: The term "student-generated content" means materials or content created by a student in the services including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of student content.

School Official: For the purposes of this DPA and pursuant to 34 CFR § 99.31(b), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of Student Data including Education Records; and (3) Is subject to 34 CFR § 99.33(a) governing the use and re disclosure of Personally Identifiable Information from Education Records.

Service Agreement: Refers to the Contract and/or Terms of Service and/or Terms of Use.

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to,

information in the student's educational record or email, first and last name, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data includes Meta Data. Student Data further includes "Personally Identifiable Information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local laws and regulations. Student Data as specified in **Exhibit "B"** is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Provider's services.

Subprocessor: For the purposes of this DPA, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its service, and who has access to Student Data.

Subscribing LEA: An LEA that was not party to the original Service Agreement and who accepts the Provider's General Offer of Privacy Terms.

Targeted Advertising: means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the usage of the operator's Internet web site, online service or mobile application by such student or the retention of such student's online activities or requests over time for the purpose of targeting subsequent advertisements. "Targeted Advertising" does not include any advertising to a student on an internet web site based on the content of the web page or in response to a student's response or request for information or feedback.

Third Party: The term "Third Party" means a provider of digital educational software or services, including cloud based services, for the digital storage, management, and retrieval of Education Records and/or Student Data, as that term is used in some state statutes. However, for the purpose of this DPA, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

EXHIBIT "D"

DIRECTIVE FOR DISPOSITION OF DATA

Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

Disposition is partial. The categories of data to be disposed of are set forth below or are found in

an attachment to this Directive:

[Insert categories of data here]

Disposition is Complete. Disposition extends to all categories of data.

2. Nature of disposition

Disposition shall be by destruction or deletion of data.

Disposition shall be by a transfer of data. The data shall be transferred to the following site as follows:

[Insert or attach special instructions]

3. Schedule of Disposition

Data shall be disposed of by the following date:

As soon as commercially practicable. By

4. Signature

Authorized Representative of LEA Date

5. Verification of Disposition of Data

Authorized Representative of Company Date

EXHIBIT "E"
GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and Education Technology joint Powers Authority ("Originating LEA") which is dated ______________________ to any other LEA ("Subscribing LEA") who accepts this General Offer of Privacy Terms ("General Offer") through its signature below. This General Offer shall extend only to privacy protections, and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the Subscribing LEA may also agree to change the data provided by Subscribing LEA to the Provider to suit the unique needs of the Subscribing LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statutes; (2) a material change in the services and products listed in the originating Service Agreement; or five (5) years after the date of Provider's signature to this Form. Subscribing LEAs should send the signed **Exhibit "E"** to Provider at the following email address:

PROVIDER: NAME

By:____ Date:________________________________

Printed Name:________________________________Title/Position:_________________________

2. Subscribing LEA

A Subscribing LEA, by signing a separate Service Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA for the term of the DPA between the

and the Provider. **PRIOR TO ITS EFFECTIVENESS, SUBSCRIBING LEA MUST DELIVER NOTICE OF ACCEPTANCE TO PROVIDER PURSUANT TO ARTICLE VI, SECTION 5. **

LEA:
BY:______________________________________Date:____ Printed Name:
______Title/Position:_________________________
SCHOOL DISTRICT NAME:____
DESIGNATED REPRESENTATIVE OF LEA:____

Name:____ Title: ________________________

Address:____ Telephone Number: ___________

Email:_______________________

EXHIBIT "F"
DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks

2/24/2020

The Education Security and Privacy Exchange ("Edspex") works in partnership with the Student Data Privacy Consortium and industry leaders to maintain a list of known and credible cybersecurity frameworks which can protect digital learning ecosystems chosen based on a set of guiding cybersecurity principles* ("Cybersecurity Frameworks") that may be utilized by Provider.

Cybersecurity Frameworks

MAINTAINING ORGANIZATION/GROUP		**FRAMEWORK(S)**
	National Institute of Standards and Technology	NIST Cybersecurity Framework Version 1.1
	National Institute of Standards and Technology	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
	International Standards Organization	Information technology - Security techniques - Information security management systems (ISO 27000 series)
	Secure Controls Framework Council, LLC	Security Controls Framework (SCF)
	Center for Internet Security	CIS Critical Security Controls (CSC, CIS Top 20)
	Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S))	Cybersecurity Maturity Model Certification (CMMC, ~FAR/DFAR)

Please visit http:// www.eds pex.org for further details about the noted frameworks.

*Cybersecurity Principles used to choose the Cybersecurity Frameworks are located here

EXHIBIT "G"
Supplemental SDPC State Terms for California

Version 1.0

This Amendment for SDPC State Terms for California **("Amendment")** is entered into on the date of full execution (the **"Effective Date")** and is incorporated into and made a part of the Student Data Privacy Agreement **("DPA")** by and between: Education Technology Joint Powers Authority, located at 5050 Barranca Parkway, Irvine, CA 92604 (the **"Local Education Agency"** or **"LEA")** and NAME, located at ADDRESS (the **"Provider").**

All capitalized terms not otherwise defined herein shall have the meaning set forth in the DPA.

WHEREAS, the Provider is providing educational or digital services to LEA, which services include: (a) cloud-based services for the digital storage, management, and retrieval of pupil records; and/or (b) digital educational software that authorizes Provider to access, store, and use pupil records; and

WHEREAS, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act **("FERPA")** at 20 U.S.C. § 1232g (34 C.F.R. Part 99); the Protection of Pupil Rights Amendment **("PPRA")** at 20 U.S.C. §1232h; and the Children's Online Privacy Protection Act **("COPPA")** at 15 U.S.C. § 6501-6506 (16 C.F.R. Part 312), accordingly, the Provider and LEA have executed the DPA, which establishes their respective obligations and duties in order to comply with such applicable laws; and

WHEREAS, the Provider will provide the services to LEA within the State of California and the Parties recognizes the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable California laws and regulations, such as the Student Online Personal Information Protection Act **("SOPIPA")** at California Bus. & Prof. Code§ 22584; California Assembly Bill 1584 **("AB 1584")** at California Education Code section 49073.1; and other applicable state privacy laws and regulations; and

WHEREAS, the Provider and LEA desire to enter into this Amendment for the purpose of clarifying their respective obligations and duties in order to comply with applicable California state laws and regulations.

NOW, THEREFORE, for good and valuable consideration, LEA and Provider agree as follows:

Term. The term of this Amendment shall expire on the same date as the DPA, unless otherwise terminated by the Parties.

Modification to **Article IV, Section** 7 **of the DPA.** Article IV, Section 7 of the DPA (Advertising Limitations) is amended by deleting the stricken text as follows:

Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data ~~(i)~~ for adaptive learning or customized student learning (including generating personalized learning recommendations)~~; or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits~~.

IN WITNESS WHEREOF, LEA and Provider execute this Amendment as of the Effective Date.

LEA: Education Technology Joint Powers Authority

By:____________________________ Date:____________________

Printed Name: Brianne Ford Title/Position: President

PROVIDER: NAME

By:____Date:________________________

Printed Name:_____________________________________Title/Position:_________________

Attachment 1: Proposal Form

Contractor Information

Firm/Contractor Name	
Primary Contact Name	
Contact Title	
Contact Email	
Contact Phone	

Write out all answers using the Proposal Form. Additional material may be submitted with the proposal as appendices. No brochures, marketing materials, or internal company documentation will be considered when scoring Proposals. In general, cross-references to the Proposal Form in additional materials will not be considered responsive. However, Ed Tech JPA will consider technical specifications for equipment and similar supplemental materials if the page numbers of the supplemental materials are clearly indicated in the relevant requirements sections and line item(s) in the pricing form. Any additional descriptive material that is used in support of any information in your proposal must be clearly identified.

Essential criteria is denoted with double asterisks (**), and green boxes. Each vendor must meet the essential criteria to be awarded a contract with Ed Tech JPA. Criteria without double asterisks in blue boxes are supplemental criteria our members may use to determine the products and services that best meet their needs.

If a Vendor offers multiple Solutions that are similar they may submit one proposal for all solutions. When the proposed Solutions offer varying features, or would otherwise elicit different responses to RFP criteria, be sure to clarify which solution the response references (responses may be broken down into different Solutions). If one proposed Solution meets the criteria but another does not, Vendors must be clear in their proposals regarding each Solution's capabilities.

Example:

3.1.1 Describe how the Solution can establish and maintain an accurate, detailed, and up-to-date **inventory of Enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. For mobile end-user devices, describe how MDM type tools can support this process, where appropriate. **
Product 1 Name (MDM): *Our MDM solution provides management and inventory control for all mobile device platforms ….(description of features)* **Product 2 Name (Server Management Solutions):** *Our team provides professional services for managing server security, scalability, and overall health …. (description of services)*

If proposed Solutions have significant differences it is recommended to submit different proposals to avoid confusion during the scoring process.

Part 1 Vendor Support and Ability to Perform

Please respond to each requirement directly and provide additional documentation as needed to support the Proposal.

1.1 Vendor Background/Qualifications:	
Instructions/Overview: Provide a brief description of Vendor’s firm(s), as well as any other firms joining with Vendor to provide services.	
History of the firm(s)	
Age of the firm(s)	
Number of employees	
Organizational structure of the firm(s)	
Length of time in the industry	
Number of office locations	
Addresses of all offices	

1.2 Vendor Contact(s)	
Instructions/Overview: Provide a list of company contacts. For each provide: name, description of role, detailed experience information and/or resume.	
Contract/sales contact	
Product manager(s)	
Other (specify)	

	Yes	No	Comments
1.3 Confirm that Vendor will meet the minimum insurance requirements specified in Appendix B. List any insurance requirements Vendor will request a waiver for, if chosen as the Selected Vendor. If the Selected Vendor fails to maintain the required insurance coverages, without a waiver approved by Ed Tech JPA and/or Participant staff, Ed Tech JPA and/or Participant may declare Vendor in breach of the Master Agreement and/or Purchase Agreement. **			
1.4 Confirm that Vendor maintains cyber insurance.			
1.5 Vendor acknowledges and agrees to all specifications listed in Sections 1 - 6 of this RFP. **			
1.6 Vendor certifies that it complies with the Civil Rights Act of 1964, and all applicable Federal and State laws and regulations relating to equal employment opportunity.			
1.7 Vendor certifies that it is, and at all times during the performance of Solution shall be, in full compliance with the provisions of the Immigration Reform and Control Act of 1986 ("IRCA") in the hiring of its employees. If awarded, Vendor shall indemnify, hold harmless and defend the Participant against any and all actions, proceedings, penalties or claims arising out of theVendor's failure to comply strictly with the IRCA.			
1.8 Vendor confirms that if any equipment delivered or supplied to a Participant as a result of this RFP is listed in the Hazardous Substance List of Regulations of the Director of Industrial Relations with the California Occupational Safety and Health Standards Board, or if			

the equipment presents a physical or health hazard as defined in the California Code of Regulations, General Industry Safety Order, Section 5194 (T8CCR), Hazard Communication, then the Vendor shall include a Material Safety Data Sheet (MSDS) with the delivery/shipment. Vendor confirms that all shipments and containers will comply with the labeling requirements of Title 49, Code of Federal Regulations by identifying the hazardous substance, name and address of manufacturer, and appropriate hazard warning regarding potential hazards.			
1.9 Vendor confirms that any Vendor representative driving motor vehicles on a Participant's school grounds will use extreme caution, especially when school is in session. Drivers will lock any gate or door to which they may have access, both when entering and/or leaving school grounds. Any unusual conditions noted by drivers such as gates or doors found unlocked and/or opened, evidence of vandalism, etc., should be immediately reported to the Participant.			

1.10 Provide a brief overview of Vendor's technical experience, qualifications, and background in providing security and IT administration products and related services for K-12 education and/or government customers. Indicate the prior experience of Vendor that is relevant to this contract. Include sufficient detail to demonstrate the relevance of such experience. Please provide specific examples of recently completed K-12 or government projects similar in size, scope and timeline to this project. Proposal should evidence Vendor's awareness of and support for the unique needs of education clients. **

1.11 Provide evidence of long-term fiscal stability. Artifacts may include fiscal reports or recent audit results that demonstrate consistent and current financial security. Financial information submitted in response to Section 1.8 will be considered proprietary information.

1.12 If Vendor does not manufacture the Solution, describe Vendor's relationship with the manufacturer of the proposed Solution. Vendors must be either manufacturers or factory authorized resellers/distributors for brands they are proposing and must be able to show proof of information.

1.13 Describe any independently awarded certifications or credentials held by the Vendor or awarded to the proposed products. Examples of appropriate certifications include those awarded by manufacturers to installation/implementation partners, certifications related to data privacy or security (e.g., FedRAMP), and certifications related to research-supported educational outcomes (e.g., Digital Promise).
Certification: Description: Year Awarded: Link to website:

1.14 Subcontractors

1.14.1 Subcontractors Information: Any subcontractors performing services against this agreement must be fully listed and detailed in the proposal submitted by Vendor. **Please keep in mind that hosting providers, such as AWS and Azure, are considered subcontractors.** State any work proposed to be provided by a subcontractor, and provide evidence of each subcontractor's capability and willingness to carry out the work. For each proposed subcontractor, include:

Firm Name	
Address	
Management contact person	
Complete description of work to be subcontracted	
Descriptive information concerning subcontractor's organization and abilities.	

	Yes	No	Comments
1.14.2 Vendor agrees to bind every subcontractor and manufacturer/reseller by the terms and conditions of this RFP, Vendor Proposal and all resulting agreements, including licensing and experience qualifications, as far as such terms and conditions are applicable to the subcontractor(s) work. If Vendor subcontracts any part of this agreement/contract, Vendor shall be fully responsible to the Participant for acts and omissions of its subcontractor and of persons either directly or indirectly employed by Vendor. Nothing contained in these contract documents shall create any contractual relation between any subcontractor and Ed Tech JPA or between any subcontractor and the Participant. **			

1.14.3 If Vendor is a reseller of the Solution, Vendor certifies that it is an authorized reseller directly through the manufacturer.			

1.15 References

	Yes	No	Comments
1.15.1 Confirm the Vendor has recent and/or active partnerships for the purchase and/or provision of services related to the Solutions called for in this RFP in at least five (5) K-12 or government organizations.**			

Provide customer references for at least five (5) K-12, postsecondary education, or government organizations currently serviced by the Vendor. Include the size of each reference organization and the scope of the project. At least three (3) of the references must be using the Solutions proposed in response to this RFP. Vendors who are not located in the United States, but who are located in a country where the GDPR governs and/or who do not perform their proposed Solutions in the United States, but whose performance is in a country where the GDPR governs (Foreign Vendors), must include at least three (3) references located within the United States that use the Solution. Each reference must include the following information:

- **Organization/Customer Name**.
- **Name, Title, and Contact Information** of an organization contact who has ongoing involvement in the Solution and is knowledgeable about the implementation.
- **Organization/Customer Size** - Indicate the number of employees, students, licenses, and stations. Indicate any additional information that may be useful in determining the size of the organization/customer.
- **Implementation Length** - Length of time from contract execution to full implementation of the system or delivery of the products.
- **Installation date** of the system if applicable (for software and or enterprise security appliances).
- **Description of in-use system** – please include details, including but not limited to, which products are currently in use by reference.
- **Vendor Project Manager**(s) for implementation and ongoing use of products and services. For product purchases (without ongoing professional services), Vendor may list the appropriate account or sales representative.

Reference #1	
Organization/Customer Name	
Name, Title & Contact information for company contact	
Organization/Customer Size - Number of employees/students/licenses	
Implementation length - from contract execution to full implementation	
Installation Date	

Description of system *include number of locations	
Vendor Project manager	

Reference #2	
Organization/Customer Name	
Name, Title & Contact information for company contact	
Organization/Customer Size - Number of employees/students/licenses	
Implementation length - from contract execution to full implementation	
Installation Date	
Description of system *include number of locations	
Vendor Project manager	

Reference #3	
Organization/Customer Name	
Name, Title & Contact information for company contact	
Organization/Customer Size - Number of employees/students/licenses	
Implementation length - from contract execution to full implementation	
Installation Date	
Description of system *include number of locations	
Vendor Project manager	

Reference #4	
Organization/Customer Name	

Name, Title & Contact information for company contact	
Organization/Customer Size - Number of employees/students/licenses	
Implementation length - from contract execution to full implementation	
Installation Date	
Description of system *include number of locations	
Vendor Project manager	

Reference #5	
Organization/Customer Name	
Name, Title & Contact information for company contact	
Organization/Customer Size - Number of employees/students/licenses	
Implementation length - from contract execution to full implementation	
Installation Date	
Description of system *include number of locations	
Vendor Project manager	

1.16 Implementation

	Yes	No	Comments
1.16.1 Vendor acknowledges and confirms compliance with all processes and requirements defined in RFP Section 2.00: Purchase Agreement Implementation Process. Identify any exceptions or deviations from the proposed project approach, site access requirements and Vendor expectations. **			
1.16.2 Vendor confirms that, for all purchases that include implementation or installation services, Vendor will provide Participants with a written			

implementation plan with specific dates no later than two weeks after receiving notification from Participants unless a later date is agreed to by both parties. **			
1.16.3 Vendor confirms that its delivery and maintenance employees shall wear distinctive company clothing and display company/employee identification, including the employee photograph and name. Vendor agrees that all Vendor employees who will be on site will adhere to applicable laws and Participants' background check and supervision requirements. All Vendor employees must check in at the administration office of each site prior to any delivery or site work. **			
1.16.4 If selected, Vendor will agree to contract language allowing mutual contract termination in whole or in part, in the event that Participant(s) does not allocate funding for the continuation of this contract or any portion thereof. In the event of termination due to non-allocation of funds, both parties shall be held without fault and there shall be no financial consequences assessed as a penalty on either party.			

1.16.5 For proposed products that include installation or implementation services, provide a general project plan for the implementation of the proposed Solution(s). Vendors that are proposing multiple, different products and services under this RFP may instead provide an overview of their project management approach and a sample project plan.**

1.16.6 For proposed products that include installation or implementation services, describe Vendor's proposed project approach, including the roles and responsibilities of project team members, required tasks and any necessary onsite work. Include a detailed list of Participant and Vendor responsibilities during the implementation process.

1.16.7 Describe Vendor capabilities to warehouse equipment for delivery and any geographic constraints. Vendor warehousing may allow for Participants to purchase in larger quantities and store in advance of individual site implementations. Specify ifVendor warehousing is an included or additional cost to the equipment costs defined in the Pricing Form.

1.16.8 Describe Vendor’s process for addressing changes that occur after the point of purchase and/or installation (e.g., warranty exchange or repair process for equipment purchases, change review and approval process for software implementations).

1.17 Training

1.17.1 Describe available training options for proposed products and services. Clearly identify which of the trainings are included with the purchase or base contract and which are provided at additional cost.

1.17.2 Describe any training resources (e.g., support library, on-demand training, or vendor-sponsored community forums) available for ongoing learning and support after implementation.

1.18 Support and Maintenance

1.18.1 Describe the scope of support provided by the Vendor for proposed products. For example, clarify whether the provider offers ongoing technical support for the proposed products or (in the case of equipment purchase) offers pre/post sales consultation, warranty repair/replacement. **

1.18.2 Describe the Vendor’s organizational structure as it relates to support. Include the number of assigned personnel and the workflow for obtaining support. For enterprise software platforms, this may include the number of support personnel and ticketing/support workflows. For equipment resellers, this may include the customer account management structure as well as available professional services to support purchased technologies. **
Organizational Structure: Number of Assigned Personnel: Workflow:

1.18.3 Describe the process for customer escalation of issues with purchased products (e.g., equipment defects or software performance issues that are significantly disrupting the organization). **

1.18.4 Provide a copy of the warranty on the proposed Solution or a narrative description of the included warranty.

1.18.5 Identify any fees associated with the return or restocking of Equipment (unrelated to warranty or performance issues).

1.18.6 For Vendor-manufactured or developed Solutions, describe the process for submission, review, escalation and development for new feature requests.

1.18.7 Describe systems in place to capture customer feedback and how that feedback is used to inform Vendor's product development, support structures, and organizational priorities.

1.18.8 If Vendor provides ongoing technical support, provide Vendor's standard expectations for response and resolution times to customer-reported issues. If expected response times differ based on the classification of the issue (i.e., severity), provide the classification criteria and corresponding response and resolution expectations.

1.18.9 State what recourse is available if the proposed Solution does not perform as quoted and the Participant is faced with loss or interruption of service.

1.18.10 Indicate the provisions for service and support if Vendor's business terminates, is subjected to a strike, or shutdown for any reason.

Part 2 Technology Requirements

Please respond to each requirement directly and provide additional documentation as needed to support the Proposal. All Vendors must meet the essential criteria defined in Section 2.1 - General Requirements. Vendors proposing equipment must additionally meet the requirements defined in section 2.2. Vendors proposing software platforms (e.g. help desk, inventory, project management software solutions), must additionally meet the essential requirements defined in section 2.3-2.6.

For any feature not included as part of the base Solution, but offered as an additional feature with an additional cost, make a note in Proposal and include the cost in Appendix C.

2.1 General Requirements (Equipment and Software)

This section is required for all Vendors

	Yes	No	Comments
2.1.1 Confirm that the Vendor's information security policies are documented and available to clients upon request.**			
2.1.2 Confirm that the Solution prevents users from accessing information on students that they are not directly involved with. If the Solution does not allow for students to be secured by teacher, grade-level at a school, and specific school, describe the different permission levels that the Solution can enforce.			
2.1.3 Confirm that Ed Tech JPA and Members may review Vendor internal and/or 3rd party security audits.			
2.1.4 Warrant that Vendor provides background checks on all employees, and/or that only employees who have undergone said background checks will have access to Participants' data. **			
2.1.5 Confirm that Vendor requires all employees to sign confidentiality and/or data handling agreements at hire.			
2.1.6 Certify that Vendor employs and will continue to employ a dedicated CISSP certified security manager, or the equivalent, to test the Solution and run ongoing checks/improvements.			
2.1.7 Vendor agrees that, even if the proposed Solution is hosted by Vendor, data housed in the Solution or submitted by Participant to Vendor remains the sole property of Participant and cannot be used in any way not explicitly approved by Participant.**			

2.1.8 Confirm that no third-party shall be given access to Participant data for any reason without explicit, written authorization from the Participant. Any third party used to support the Solution must be identified as a designated subcontractor in the RFP response. **			

2.1.9 Provide a description of Vendor policy regarding storage, retention, and distribution of data. State Vendor data non-release policy.

2.1.10 Explain internal Vendor company protocols regarding the handling of client data.

2.1.11 The Solution shall effectively secure and protect student information. Please describe the security measures (physical and technological) taken to protect data.

2.2 Equipment Requirements

This section is required for all Vendors submitting Proposals that include equipment/hardware offerings.

	Yes	No	Comments
2.2.1 Confirm that all proposed equipment consists of new and original components and Participants shall be the first user of the equipment. *Vendor shall not provide “remanufactured equipment” i.e. equipment that has been factory disassembled to a predetermined standard, then reassembled by using new parts and some used or recycled components.			
2.2.2 Confirm that Quotes shall include all costs including shipping and handling and equipment shall be delivered (F.O.B.) to Participant address(es).			

2.2.3 Confirm that all proposed equipment consists of new and original components and Participants shall be the first user of the equipment. Vendor shall not provide “remanufactured equipment” i.e. equipment that has been factory disassembled to a predetermined standard, then reassembled by using new parts and some used or recycled components. **

2.2.4 Provide a copy of the warranty on the proposed Solution or a narrative description of the provisions of the warranty.

2.2.5 Describe Vendor’s, Manufacturer’s and Participant’s respective roles in resolving warranty and equipment performance issues. Please include any advocacy, documentation, or other support provided by Vendor to resolve issues. **

2.2.6 Confirm that all replacement and equipment provided to resolve warranty issues will be new equipment (not refurbished). If refurbished equipment is used, provide details as to when Vendor shall provide refurbished equipment vs. new equipment and what performance guarantees are available to Participants.

2.2.7 Provide technical specifications for proposed equipment. Vendors proposing multiple products may attach separate documentation of the technical specifications of available equipment. In that case, please provide a list of the proposed equipment with page references for the technical specifications. Links to online catalogs and manufacturer websites are only acceptable if the Vendor is proposing a catalog discount offering (e.g., 20% off MSRP for all products sold under a specific brand name).

2.3 Software Platform Requirements

This section is required for all Vendors submitting Proposals that include software platform offerings (e.g. help desk, inventory, project management software solutions).

2.3.1 Provide information regarding the Solution database platform and versions supported.

2.3.2 Specify whether the Solution is Vendor-hosted (web/cloud-based) or Participant-hosted (on-premise). **

2.3.2.1 If the Solution is on-premise, specify all hardware required to support the Solution.

2.3.2.2 If the Solution is on-premise, confirm that the Solution can be run in a Virtualized environment (VM Ware, Hyper V).

2.3.2.3 If the Solution is web/cloud-based, describe what measures have been taken to ensure resiliency/high availability.

2.3.2.4 If the Solution is web/cloud-based, describe any browser or application requirements including: supported browsers and minimum versions, dependencies on third-party software. Please note any browser specific limitations to the functionality provided by the Solution.

2.3.3 Provide details regarding Vendor needs and expectations for remote access to systems and open ports required for communication and data exchange between system components. **

2.3.4 Describe Vendor process for testing and releasing software updates, and providing for business continuity during major upgrades. Describe expectations of Participant staff to apply upgrades for Solution.

2.3.5 Describe the typical frequency of software updates on an annual basis and whether software updates are required at these intervals or if they are included/or optional. Describe how Participants are notified of new software upgrades and tools available.

2.3.6 Describe what features are embedded in the Solution to ensure that Solution and all Vendor-supplied content meet WCAG 2.0AA requirements and provide access to individuals with disabilities.**

2.3.7 Describe any features available in the Solution to identify and remediate accessibility issues with Participant-provided content (if applicable).

2.3.8 Describe Provider’s approach to assessing usability and navigability of the Solution (e.g., periodic third-party usability studies, collection of user feedback, use of navigation/user activity data, design review processes).

2.4 Performance and Reliability (Software)

This section is required for all Vendors submitting Proposals that include software platform offerings (e.g. help desk, inventory, project management software solutions).

2.4.1 Describe performance monitoring or other tools/techniques used to ensure consistent response times and availability of the Solution.

2.4.2 Describe Vendor recommended/used database backup, system recovery, and failover capabilities to minimize the system downtime and risk of data loss.

2.4.3 State uptime for the Solution for the past three (3) years. Scheduled maintenance that renders the Solution unavailable for typical usage, should be counted as an outage. Describe process for maintenance, including communications and Solution availability during scheduled maintenance. Define uptime commitments included in Vendor’s service level agreement.**

2.4.4 Provide a list of any site-wide outages over the past two years. Include the duration of the outage and an impact statement listing the services affected.**

2.4.5 Describe any data loss or data corruption that occurred in the past three (3) years. Identify any customers that experienced lost or compromised data and the source of the issue.**

2.4.6 Describe Vendor support for disaster recovery of the complete Solution in the instance of data corruption, complete data failure, complete server failure, or complete site failure. Provide evidence of comprehensive disaster recovery planning.

2.4.7 Describe how Vendor anticipates and provides for increases in data storage needs, increasing size and scope of data sets on-line, and increasing number of users. Provide an overview of how Vendor scales both infrastructure and support personnel to meet necessary demand.

2.4.8 If on-premise installation is recommended, provide all technical documentation including minimum requirements, database sizing recommendations, and Solution architecture and installation.

2.5 Upgrades and Maintenance (Software)

This section is required for all Vendors submitting Proposals that include software platform offerings (e.g. help desk, inventory, project management software solutions).

2.5.1 Confirm anticipated Solution availability (ideally 24/7, 365 days per year). Provide details related to scheduled maintenance windows and precautions taken to minimize service disruption due to planned maintenance.**

2.5.2 Clarify whether Vendor will host dedicated, separate production, test and training environments for Participants under this agreement. Participants may request a testing database that is refreshed nightly from production data, where new releases can be previewed and modifications tested prior to application to production. A training database should provide a de-identified/scrambled data set for use in conducting training and developing internal training documents.

2.5.3 If a dedicated, separate test environment is not provided as part of the Solution, describe Vendor's recommended strategy for safely applying and testing configuration changes and/or large-scale data changes (e.g., modifying an import file).

2.5.4 Provide details on maintenance service arrangements for the proposed Solution and the cost for any alternative available including maintenance contracts and per-call maintenance cost. Please also include all costs in Appendix C.

2.6 Data and Interoperability (Software)

This section is required for all Vendors submitting Proposals that include software platform offerings (e.g. help desk, inventory, project management software solutions).

2.6.1 Please describe how Vendor’s proposed Solution supports Participants’ full access to extract their user-generated, system and usage data.**

2.6.2 Please specify which platforms Vendor’s proposed Solution integrates with for authentication/authorization (Active Directory, Google Single Sign On, etc.). **

2.6.3 Provide a list of other products for which the proposed Solution has a pre-built integration with. (Examples: Aeries, Powerschool, Infinite Campus, Bitech, Business Plus, Schoolloop, SchoolMessenger, Blackboard). For each, please briefly describe the level of integration and how frequently the Solution can pull/refresh data from these data sources. For systems that rely on data FROM the proposed product(s), specify any limitations on the number, frequency or scope of scheduled extracts that Participant agencies can create and use. **

2.6.4 Describe Vendor’s data integration and loading process; please also include sample file layouts. **

2.6.5 Describe support for creating custom, scheduled imports and exports.

2.6.6 Describe the capabilities of the Solution to provide bulk imports and exports.

2.6.7 ** Describe the Solution’s approach to interoperability with other data systems.

2.6.7.1 Explain the process and tools available (ex: API) for Participants to integrate the Solution with other data systems.

2.6.7.2 Describe whether the Solution adheres to common standards (ex: Ed-Fi, One-Roster) and /or leverages third-party integration options (ex: Clever, Classlink) to improve interoperability.

2.6.7.3 If the Solution does not utilize or conform to any common standards, describe how Vendor guarantees data interoperability between Solution and various Participant existing systems.

Parts 3 & 4 Functionality and Usability

These sections should include an in-depth description of the proposed Solution(s). **Vendors may respond and be awarded to *one or more* Solution Domain, and are not required to respond to all domains** (for example, a vendor that offers only Malware Defenses and not Account Management may respond only to the Malware Defenses section and be awarded for that section only).

Please indicate below which Solution Domain(s) Vendor is proposing in response to this RFP. Mark "Y" in the Included in Proposal Column for any domain for which the Vendor has at least one proposed Solution. In the corresponding requirements section, respond to each requirement with a narrative explanation of how the proposed Solution(s) meet the stated requirement.

Sections 3.1 through 3.18 of this RFP were adapted with permission from version 8 of the CIS Controls developed by the Center for Internet Security (cisecurity.org). CIS provides expert guidance and well-defined security standards for public agencies. The CIS Controls and corresponding safeguards articulate best practices related to systems, configuration, policies, and procedures associated with a wide variety of technologies. This RFP is intended to solicit a variety of offerings from Vendors to assist Participants in addressing security concerns, including software, equipment and professional services. Each of the requirements in the RFP based on the CIS Controls are described as a desired outcome (the control/safeguard). Vendors should respond to the requirement by describing, in detail, how their products and/or services would support the Participant in implementing that control. For example, for controls related to policies and documentation, Vendors may offer templates and consulting services to help Participants develop and implement appropriate security policies. For controls related to network monitoring, Vendors may offer specific hardware and software products and/or security monitoring and incident response as a service.

Vendors are not required to respond to all subsections in the Functionality and Usability Section of this RFP. Instead, Vendors should respond only to those subsections for which they are proposing Solutions. The introductory text of each subsection includes examples of products and services that may address the requirements within that subsection. Please use the chart below to indicate which subsections are included in the Vendor's Proposal.

<table>
<tr><th colspan="2"><b>Security</b>
<i>Note: Each of the Security Requirements Sections aligns to the CIS Controls and Safeguards (version 8).</i></th></tr>
<tr><td>Solution Domain</td><td>Included in Proposal (Y/N)</td></tr>
<tr><td>3.1 Inventory and Control of Enterprise Assets</td><td></td></tr>
<tr><td>3.2 Inventory and Control of Software Assets</td><td></td></tr>
<tr><td>3.3 Data Protection</td><td></td></tr>
<tr><td>3.4 Secure Configuration of Enterprise Assets and Software</td><td></td></tr>
<tr><td>3.5 Account Management</td><td></td></tr>
<tr><td>3.6 Access Control Management</td><td></td></tr>
<tr><td>3.7 Continuous Vulnerability Management</td><td></td></tr>
<tr><td>3.8 Audit Log Management</td><td></td></tr>
<tr><td>3.9 Email and Web Browser Protections</td><td></td></tr>
<tr><td>3.10 Malware Defenses</td><td></td></tr>
<tr><td>3.11 Data Recovery Solutions</td><td></td></tr>
<tr><td>3.12 Network Infrastructure Management</td><td></td></tr>
<tr><td>3.13 Network Monitoring and Defense</td><td></td></tr>
<tr><td>3.14 Security Awareness and Skills Training</td><td></td></tr>
<tr><td>3.15 Service Provider Management</td><td></td></tr>
<tr><td>3.16 Application Software Security</td><td></td></tr>
<tr><td>3.17 Incident Response Management</td><td></td></tr>
<tr><td>3.18 Penetration Testing</td><td></td></tr>
<tr><td>3.19 Security Services</td><td></td></tr>
<tr><td>3.20 Campus Safety (Facility Security)</td><td></td></tr>
<tr><th colspan="2"><b>Information Technology (IT) Administration</b></th></tr>
<tr><td>Solution Domain</td><td>Included in Proposal (Y/N)</td></tr>
<tr><td>4.1 Help Desk</td><td></td></tr>
<tr><td>4.2 Project Management</td><td></td></tr>
<tr><td>4.3 Student Safety and Classroom Management</td><td></td></tr>
</table>

Security

[Insert language referencing CIS Controls and methodology for award. Clarify that vendors may propose multiple solutions or products to meet the needs].

3.1 Inventory and Control of Enterprise Assets

Proposed Solution(s): List all equipment, software, services and other products included in the Proposal that are offered in response to the requirements in this section. For each item or collection of items, add a Solution Name and list the corresponding line number(s) from the Pricing Form. If you have provided additional technical literature or other reference materials for the Proposed Solution(s), include the page number(s) where the documentation can be found in the Proposal.

Examples of Proposed Solutions: For this section, Providers may consider proposing inventory, asset management, device management, mobile device management, automated device discovery, and other Solutions that meet the associated requirements. If the Provider proposal includes a Solution with multiple components, configuration options, or pricing tiers, the Solution may be listed on one line in the table below with the appropriate references to the line numbers corresponding to each of the options and components included on the pricing form (e.g., Proposed Solution - *Brand Name MDM,* Line Number(s) - *5-25*).

Proposed Solution Name	Line Number(s) *From Pricing Form*	Page Number(s) *Reference Material*

3.1.0 Describe how the Solution can **actively manage (inventory, track, and correct) Enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to support Participant in accurately knowing the totality of assets that need to be monitored and protected within the Enterprise. Please be sure to include how the Solution also supports identifying unauthorized and unmanaged assets to remove or remediate. **

3.1.1 Describe how the Solution can establish and maintain an accurate, detailed, and up-to-date **inventory of Enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. For mobile end-user devices, describe how MDM type tools can support this process, where appropriate. **

3.1.1.1 Describe how the Solution can ensure the inventory records the network address (if static), hardware address, machine name, Enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network.

3.1.1.2 Describe how the Solution can ensure that this inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments.

3.1.1.3 Describe how the Solution can support Participants' ability to review and update the inventory of all Enterprise assets bi-annually, or more frequently.

3.1.1.4 Describe how the Solution supports the inclusion of assets that are regularly connected to the Enterprise's network infrastructure, even if they are not under control of the Enterprise.

3.1.1.5 Describe features in the Solution designed to help Participants in efficiently and actively managing (inventory, track, and correct) all Enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments.

3.1.1.6 Describe how the Solution can also support identifying unauthorized and unmanaged assets to remove or remediate.

3.1.2 Describe how the Solution can support a Participant's process to address unauthorized assets. Please also describe how a Participant may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.

3.1.3 Describe how the Solution provides an active discovery tool to identify assets connected to the Enterprise's network. Describe how the Solution can be configured to support the active discovery tool to execute daily, or more frequently.

3.1.4 Describe how the Solution can support Participants' use of DHCP logging on all DHCP servers or Internet Protocol (IP) address management tools to update the Enterprise's asset inventory. Review and use logs to update the Enterprise's asset inventory weekly, or more frequently.

3.1.5 Describe how the Solution can support Participants' use of a passive discovery tool to identify assets connected to the Enterprise's network. Please also describe how Participants can use the Solution to review and use scans to update the Enterprise's asset inventory.

3.1.6 Describe what additional inventory systems the Solution integrates with and how those can be used to import and/or consolidate inventory records.

3.1.7 Describe how the Solution integrates with help desk solutions or service/repair ticketing to record and display request history by inventory item.

3.1.8 Describe what exporting capabilities are available in the Solution to support inventory management (ie: what formats data can be exported, and what type of data can be exported).

3.1.9 Describe features available in the Solution designed to maintain an accurate inventory and support lifecycle management of devices that are predominantly used off-site (outside of Participant's network).

3.1.10 Describe features available in the Solution designed to detect potentially lost, stolen or unused assets (e.g., reporting and alerting tools related to device activity/stagnation, last user, last location).

3.1.11 Describe any additional features of the Solution that support inventory and control of Enterprise assets.

3.2 Inventory and Control of Software Assets

Proposed Solution(s): List all equipment, software, services and other products included in the Proposal that are offered in response to the requirements in this section. For each item or collection of items, add a Solution Name and list the corresponding line number(s) from the Pricing Form. If you have provided additional technical literature or other reference materials for the Proposed Solution(s), include the page number(s) where the documentation can be found in the Proposal.

Examples of Proposed Solutions: For this section, Providers may consider proposing software inventory, management, deployment, usage, licensing, monitoring or other software management and security solutions. If the Provider proposal includes a Solution with multiple components, configuration options, or pricing tiers, the Solution may be listed on one line in the table below with the appropriate references to the line numbers corresponding to each of the options and components included on the pricing form (e.g., Proposed Solution - *Brand Name MDM,* Line Number(s) - *5-25*).

Proposed Solution Name	Line Number(s) *From Pricing Form*	Page Number(s) *Reference Material*

3.2.0 Describe how the Solution can support Participants in actively managing (inventory, track, and correct) software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

**3.2.1 Describe how the Solution can support Participants to establish and maintain a detailed inventory of licensed software installed on Enterprise assets. **

3.2.1.1 Confirm whether the Solution can include the following attributes for all software programs (where applicable): software title, publisher, initial install/use date, expiration date (or contract end date), and business purpose, Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date.

3.2.1.2 Describe how the Solution can support Participants in reviewing and updating the software at regular intervals (at least bi-annually).

3.2.2 Describe how the Solution can support Participants to ensure that only currently supported software is designated as authorized in the software inventory for Enterprise assets.

3.2.2.1 Describe how the Solution supports Participants in identifying software that may be unsupported, but necessary for the fulfillment of the Enterprise’s mission. Describe how the Solutions supports Participants in developing and/or documenting mitigation strategies and residual risk acceptance for unsupported software.

3.2.2.2 Describe how the Solution can provide a software list to Participants for verification of software support (at least monthly).

3.2.2.3 Describe how the Solution can identify unauthorized and unmanaged assets to remove or remediate.

3.2.3 Describe how the Solution can ensure that unauthorized software is either removed from use on Enterprise assets or receives a documented exception. Please also describe any tools to support Participants’ to review and remediation of unauthorized software on a regular basis.

3.2.4 Describe how the Solution supports automated discovery and documentation of installed software.

3.2.5 Describe technical controls included in the Solution, such as application allowlisting, designed to ensure that only authorized software can execute or be accessed. Please also describe any tools available to support Participant to reassess authorized software bi-annually, or more frequently.

3.2.6 Describe technical controls available to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc. files, are allowed to load into a system process. Please also describe how the Solution can support Participants to block unauthorized libraries from loading into a system process.

3.2.7 Describe technical controls available, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Please also describe any tools available block unauthorized scripts from executing.

3.2.8 Describe what additional features the Solution has to inventory and manage software contracts (including alerting to upcoming expiration dates, lifecycle management and version control, and disallowing use after contract expiration).

3.2.9 Describe any additional features of the Solution that support inventory and control of software assets.

3.3 Data Protection

Proposed Solution(s): List all equipment, software, services and other products included in the Proposal that are offered in response to the requirements in this section. For each item or collection of items, add a Solution Name and list the corresponding line number(s) from the Pricing Form. If you have provided additional technical literature or other reference materials for the Proposed Solution(s), include the page number(s) where the documentation can be found in the Proposal.

Examples of Proposed Solutions: For this section, Providers may consider proposing products and services that support the identification, classification, management, retention and destruction of sensitive data. Solutions could include encryption tools, solutions for managing access to data and detecting breaches, solutions for secure transfer of data, e-Waste services (including data destruction), solutions that support data retention and lifecycle management, or any other product or service related to data protection. If the Provider proposal includes a Solution with multiple components, configuration options, or pricing tiers, the Solution may be listed on one line in the table below with the appropriate references to the line numbers corresponding to each of the options and components included on the pricing form (e.g., Proposed Solution - *Brand Name Document Management System,* Line Number(s) - *5-25*).

Proposed Solution Name	Line Number(s) *From Pricing Form*	Page Number(s) *Reference Material*

3.3.0 Describe how the Solution can support Participants to develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.

**3.3.1 Describe how the Solution can support Participants to establish and maintain a data management process. **

3.3.1.1 In the process, address how the Solution supports classifying data and recording information related to data sensitivity, data owner, authoritative data source, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the Enterprise.

3.3.1.2 Describe how the Solution can support Participants to review and update documentation annually, or when significant Enterprise changes occur that could impact this Safeguard.

3.3.2 Describe how the Solution can support Participants to establish and maintain a data inventory, based on the Enterprise's data management process, including the Inventory of sensitive data, at a minimum. Please also describe any tools available to support Participants' to review and update inventory annually, at a minimum, with a priority on sensitive data.

3.3.3 Describe how the Solution can support Participants to configure data access control lists based on a user's need to know. Please also describe tools within the Solution to support Participants to apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.

3.3.4 Describe how the Solution can support Participants to retain data according to the Enterprise's data management process. Data retention must include both minimum and maximum timelines.

3.3.5 Describe how the Solution can support Participants to securely dispose of data as outlined in the Enterprise’s data management process. The disposal process and method must be commensurate with the data sensitivity.

3.3.6 Describe how the Solution can support Participants to encrypt data on end-user devices containing sensitive data.

3.3.7 Describe how the Solution can support maintenance of an overall data classification scheme. This may use labels, such as “Sensitive,” “Confidential,” and “Public,” and support the classification of data according to those labels. Please also describe how the Solution can support Participants to review and update the classification scheme annually, or when significant Enterprise changes occur that could impact this Safeguard.

3.3.8 Describe how the Solution can support documentation of data flows. Data flow documentation includes service provider data flows and should be based on the Enterprise’s data management process. Please also describe any tools to support Participants to review and update documentation annually, or when significant Enterprise changes occur that could impact this Safeguard.

3.3.9 Describe how the Solution supports encryption of data on removable media.

3.3.10 Describe how the Solution can support encryption of sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).

3.3.11 Describe how the Solution can support encryption of sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.

3.3.12 Describe how the Solution can support segmentation of data processing and storage based on the sensitivity of the data. Please also describe any tools to prevent processing sensitive data on Enterprise assets intended for lower sensitivity data.

3.3.13 Describe how the Solution can support Participants to implement an automated tool, such as a host-based Data Loss Prevention (DLP) tool to identify all sensitive data stored, processed, or transmitted through Enterprise assets, including those located onsite or at a remote service provider, and update the Enterprise's sensitive data inventory.

3.3.14 Describe how the Solution can support logging of and/or analysis of logs related to sensitive data access, including modification and disposal.

3.3.15 Describe how Participants can interact with and/or export logs. Provide screenshots to demonstrate search features, available reporting tools and file export layouts.

3.3.16 Describe any additional features of the Solution that support data governance and data protection.

3.4 Secure Configuration of Enterprise Assets and Software

Proposed Solution(s): List all equipment, software, services and other products included in the Proposal that are offered in response to the requirements in this section. For each item or collection of items, add a Solution Name and list the corresponding line number(s) from the Pricing Form. If you have provided additional technical literature or other reference materials for the Proposed Solution(s), include the page number(s) where the documentation can be found in the Proposal.

Examples of Proposed Solutions: For this section, Providers may consider proposing tools that support secure and repeatable configuration of network devices, device and infrastructure policy management tools, DNS servers (or hosting services), firewalls, administrator password management tools, and other Solutions that meet the associated requirements. If the Provider proposal includes a Solution with multiple components, configuration options, or pricing tiers, the Solution may be listed on one line in the table below with the appropriate references to the line numbers corresponding to each of the options and components included on the pricing form (e.g., Proposed Solution - *Brand Name DNS Servers and Configuration Options,* Line Number(s) - *5-25*).

Proposed Solution Name	Line Number(s)	Page Number(s)

	From Pricing Form	*Reference Material*

**3.4.0 Describe how the Solution can support Participants to establish and maintain the secure configuration of Enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications). **

3.4.1 Please describe any tools to support Participants to review and update configuration documentation annually, or when significant Enterprise changes occur that could impact this Safeguard.

3.4.2 Describe how the Solution can support Participants to establish and maintain a secure configuration process for network devices. Please also describe any tools to support Participants to review and update documentation annually, or when significant Enterprise changes occur that could impact this Safeguard.

3.4.3 Describe how the Solution can support Participants to configure automatic session locking on Enterprise assets after a defined period of inactivity.

3.4.4 Describe how the Solution can support Participants to implement and manage a firewall on servers, where supported.

3.4.5 Describe how the Solution can support Participants to implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

3.4.6 Describe how the Solution can support Participants to securely manage Enterprise assets and software. Example implementations include managing configuration through

version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS).

3.4.7 Describe how the Solution can support Participants to manage default accounts on Enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.

3.4.8 Describe how the Solution can support Participants to uninstall or disable unnecessary services on Enterprise assets and software, such as an unused file sharing service, web application module, or service function.

3.4.9 Describe how the Solution can support Participants to configure trusted DNS servers on Enterprise assets. Example implementations include: configuring assets to use Enterprise-controlled DNS servers and/or reputable externally accessible DNS servers.

3.4.10 Describe how the Solution can support Participants to enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices.

3.4.11 Describe how the Solution can support Participants to remotely wipe Enterprise data from Enterprise-owned portable end-user devices when deemed appropriate such as lost or stolen devices, or when an individual no longer supports the Enterprise.

3.4.12 Describe how the Solution can support Participants to ensure separate Enterprise workspaces are used on mobile end-user devices to separate Enterprise applications and data from personal applications and data.

3.4.13 Describe any additional features of the Solution that support secure configuration of Enterprise assets and software.

3.5 Account Management

Proposed Solution(s): List all equipment, software, services and other products included in the Proposal that are offered in response to the requirements in this section. For each item or collection of items, add a Solution Name and list the corresponding line number(s) from the Pricing Form. If you have provided additional technical literature or other reference materials for the Proposed Solution(s), include the page number(s) where the documentation can be found in the Proposal.

Examples of Proposed Solutions: For this section, Providers may consider proposing identity management, identity/directory systems (including hosted systems), user account audit and monitoring services, password management, and other Solutions that meet the associated requirements. If the Provider proposal includes a Solution with multiple components, configuration options, or pricing tiers, the Solution may be listed on one line in the table below with the appropriate references to the line numbers corresponding to each of the options and components included on the pricing form (e.g., Proposed Solution - *Brand Name Identity Management Solution and Optional Modules,* Line Number(s) - *5-25*).

Proposed Solution Name	Line Number(s) *From Pricing Form*	Page Number(s) *Reference Material*

**3.5.0 Describe services, processes, and tools included in the Solution to support assignment and management of credentials for user accounts, including end-user accounts, administrator accounts, service accounts, to Enterprise assets and software. **

3.5.1 Describe how the Solution can support Participants to establish and maintain an inventory of all accounts managed in the Enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Please also describe any tools to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.

3.5.2 Describe how the Solution can enforce use of unique passwords for all Enterprise assets.

3.5.2.1 Describe how password policies may be differentiated by user or account attributes (e.g., differentiated complexity requirements for younger students, or whether the user is using MFA).

3.5.3 Describe how the Solution can support Participants to delete or disable any dormant accounts after a specified period of inactivity.

3.5.4 Describe how the Solution can support Participants to restrict administrator privileges to dedicated administrator accounts on Enterprise assets. Please also describe any tools that can support Participants to conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.

3.5.5 Describe how the Solution can support Participants to establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose. Please also describe any tools that can support Participants to perform service account reviews to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.

3.5.6 Describe how the Solution can support Participants to centralize account management through a directory or identity service.

3.5.7 Describe how the Solution identifies suspended accounts.

3.5.8 Describe any additional features of the Solution that support account management.

3.6 Access Control Management

Proposed Solution(s): List all equipment, software, services and other products included in the Proposal that are offered in response to the requirements in this section. For each item or collection of items, add a Solution Name and list the corresponding line number(s) from the Pricing Form. If you have provided additional technical literature or other reference materials for the Proposed Solution(s), include the page number(s) where the documentation can be found in the Proposal.

Examples of Proposed Solutions: For this section, Providers may consider proposing identity management, account lifecycle management solutions, mult-ifactor authentication (MFA) solutions, single-sign on portals, Virtual Private Network (VPN solutions), user account audit and monitoring services, password management, and other Solutions that meet the associated requirements. If the Provider proposal includes a Solution with multiple components, configuration options, or pricing tiers, the Solution may be listed on one line in the table below with the appropriate references to the line numbers corresponding to each of the options and components included on the pricing form (e.g., Proposed Solution - *Brand Name Identity Management Solution and Optional Modules,* Line Number(s) - *5-25*).

Proposed Solution Name	Line Number(s) *From Pricing Form*	Page Number(s) *Reference Material*

**3.6.0 Describe processes and tools included in the Solution to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for Enterprise assets and software. **

3.6.1 Describe how the Solution can support Participants to establish and follow a process, preferably automated, for granting access to Enterprise assets upon new hire, rights grant, or role change of a user.

3.6.2 Describe how the Solution can support Participants to establish and follow a process, preferably automated, for revoking access to Enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary for Participants to preserve audit trails.

3.6.3 Describe how the Solution can support Participants to require specific applications to enforce Multi-Factor Authentication (MFA), where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.

3.6.4 Describe how the Solution can support Participants to require MFA for remote network access.

3.6.5 Describe how the Solution can support Participants to require MFA for all administrative access accounts, where supported, on all Enterprise assets, whether managed on-site or through a third-party provider.

3.6.6 Describe how the Solution can support Participants to establish and maintain an inventory of the Enterprise's authentication and authorization systems, including those hosted on-site or at a remote service provider. Please also describe any tools that can support Participants to review and update the inventory, at a minimum, annually, or more frequently.

3.6.7 Describe how the Solution can support Participants to centralize access control for all Enterprise assets through a directory service or SSO provider, where supported.

3.6.8 Describe how the Solution can support Participants to define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the Enterprise to successfully carry out its assigned duties. Please also describe any tools that can support Participants to perform access control reviews of Enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.

3.6.9 Describe how the Solution supports Participants in implementing, maintaining and managing an Enterprise-level MFA.

3.6.10 Describe any additional features of the Solution that support access control management.

3.7 Continuous Vulnerability Management

Proposed Solution(s): List all equipment, software, services and other products included in the Proposal that are offered in response to the requirements in this section. For each item or collection of items, add a Solution Name and list the corresponding line number(s) from the Pricing Form. If you have provided additional technical literature or other reference materials for the Proposed Solution(s), include the page number(s) where the documentation can be found in the Proposal.

Examples of Proposed Solutions: For this section, Providers may consider proposing patch and update management solutions, vulnerability scanning, vulnerability and remediation services and platforms, and any other Solutions related to vulnerability management. If the Provider proposal includes a Solution with multiple components, configuration options, or pricing tiers, the Solution may be listed on one line in the table below with the appropriate references to the line numbers corresponding to each of the options and components included on the pricing form (e.g., Proposed Solution - *Brand Name Vulnerability Scanner,* Line Number(s) - *5-25*).

Proposed Solution Name	Line Number(s) *From Pricing Form*	Page Number(s) *Reference Material*

**3.7.0 Describe how the Solution can support Participants in assessing and tracking vulnerabilities on all Enterprise assets within the Enterprise's infrastructure, in order to remediate, and minimize, the window of opportunity for attackers. Please also describe any tools that can support Participants to monitor public and private industry sources for new threat and vulnerability information. **

3.7.1 Describe how the Solution can support Participants to establish and maintain a documented vulnerability management process for Enterprise assets. Please also describe any tools that can support Participants to review and update documentation annually, or when significant Enterprise changes occur that could impact this Safeguard.

3.7.2 Describe how the Solution can support Participants to establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.

3.7.3 Describe how the Solution can support Participants to perform *operating system* updates on Enterprise assets through automated patch management on a monthly, or more frequent, basis.

3.7.4 Describe how the Solution can support Participants to perform *application* updates on Enterprise assets through automated patch management on a monthly, or more frequent, basis.

3.7.5 Describe how the Solution can support Participants to perform automated vulnerability scans of internal Enterprise assets on a quarterly, or more frequent, basis; conducting both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.

3.7.6 Describe how the Solution can support Participants to perform automated vulnerability scans of externally-exposed Enterprise assets using a SCAP-compliant vulnerability scanning tool. Please also describe any tools that can support Participants to perform scans on a monthly, or more frequent, basis.

3.7.7 Describe how the Solution can support Participants to remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.

3.7.8 Describe any capabilities within the Solution to monitor third-party websites and applications for exposure of Participant confidential information, including personnel data, student data, financials data and/or compromised usernames and passwords.

3.7.9 Describe how the Solution supports source validation for manually installed patches and updates (e.g., ensuring patches are downloaded from known-legitimate manufacturer/provider websites).

3.7.10 Describe any additional features of the Solution that support continuous vulnerability management.

3.8 Audit Log Management

Proposed Solution(s): List all equipment, software, services and other products included in the Proposal that are offered in response to the requirements in this section. For each item or collection of items, add a Solution Name and list the corresponding line number(s) from the Pricing Form. If you have provided additional technical literature or other reference materials for the Proposed Solution(s), include the page number(s) where the documentation can be found in the Proposal.

Examples of Proposed Solutions: For this section, Providers may consider proposing audit logging and log aggregation solutions, investigative tools to detect breaches and assess incidents, security monitoring tools, Google Workspace, Office 365 and other cloud platform monitoring platforms, and other Solutions that meet the associated requirements. If the Provider proposal includes a Solution with multiple components, configuration options, or pricing tiers, the Solution may be listed on one line in the table below with the appropriate references to the line numbers corresponding to each of the options and components included on the pricing form (e.g., Proposed Solution - *Brand Name Log Aggregation Software and Services,* Line Number(s) - *5-25*)

Proposed Solution Name	Line Number(s) *From Pricing Form*	Page Number(s) *Reference Material*

3.8.0 Describe how the Solution can support Participants to collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.

3.8.1 Describe how the Solution can support Participants to establish and maintain an audit log management process that defines the Enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for Enterprise assets. Please also describe tools that can support Participants to review and update documentation annually, or when significant Enterprise changes occur that could impact this Safeguard.

3.8.2 Describe how the Solution collects audit logs. Please also describe tools that can support Participants to ensure that logging, per the Enterprise's audit log management process, has been enabled across Enterprise assets.

3.8.3 Describe how the Solution can support Participants to ensure that logging destinations maintain adequate storage to comply with the Enterprise's audit log management process.

3.8.4 Describe how the Solution can support Participants to standardize time synchronization. Please also describe the Solution's capacity to support Participants to configure at least two synchronized time sources across Enterprise assets, where supported.

3.8.5 Describe how the Solution can support Participants to configure detailed audit logging for Enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.

3.8.6 Describe how the Solution can support Participants to collect DNS query audit logs on Enterprise assets, where appropriate and supported.

3.8.7 Describe how the Solution can support Participants to collect URL request audit logs on Enterprise assets, where appropriate and supported.

3.8.8 Describe how the Solution can support Participants to collect and analyze command-line audit logs. Example implementations include collecting audit logs using PowerShell, BASH, and remote administrative terminals.

3.8.9 Describe how the Solution can support Participants to centralize audit log collection and retention across Enterprise assets.

3.8.10 Describe how the Solution can support Participants to retain audit logs across Enterprise assets for a minimum of ninety (90) days.

3.8.11 Describe how the Solution can support Participants to conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Please also describe tools that can support Participants to conduct reviews on a weekly, or more frequent, basis.

3.8.12 Describe how the Solution can support Participants to collect service provider logs, where supported. Example implementations include collecting authentication and authorization events, data creation and disposal events, and user management events.

3.8.13 Describe capabilities within the Solution to correlate logs, manage data, identify patterns, and conduct searches in a reasonable time frame.

3.8.14 Describe the format data may be exported in (Ex: CSV).

3.8.15 Describe any additional features of the Solution that support audit log management.

3.9 Email and Web Browser Protections

Proposed Solution(s): List all equipment, software, services and other products included in the Proposal that are offered in response to the requirements in this section. For each item or collection of items, add a Solution Name and list the corresponding line number(s) from the Pricing Form. If you have provided additional technical literature or other reference materials for the Proposed Solution(s), include the page number(s) where the documentation can be found in the Proposal.

Examples of Proposed Solutions: For this section, Providers may consider proposing firewall solutions, web filtering, DNS filtering, email security and policy management, and other Solutions that meet the associated requirements. If the Provider proposal includes a Solution with multiple components, configuration options, or pricing tiers, the Solution may be listed on one line in the table below with the appropriate references to the line numbers corresponding to each of the options and components included on the pricing form (e.g., Proposed Solution - *Brand Name Filtering Solution and Add-On Module Options,* Line Number(s) - *5-25*).

Proposed Solution Name	Line Number(s) *From Pricing Form*	Page Number(s) *Reference Material*

**3.9.0 Describe how the Solution can support Participants to improve protections and detections of threats from email and/or web vectors. **

3.9.1 Describe how the Solution can support Participants to ensure only fully supported browsers and email clients are allowed to execute in the Enterprise.

3.9.1.1 Describe how the Solution supports restricting or limiting use of internet browsers and email clients by version.

3.9.2 Describe how the Solution can support Participants to use DNS filtering services on all Enterprise assets to block access to known malicious domains.

3.9.3 Describe how the Solution can support Participants to enforce and update network-based URL filters to limit an Enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Please also describe tools that can support Participants to enforce filters for all Enterprise assets.

3.9.4 Describe how the Solution can support Participants to restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.

3.9.5 To lower the chance of spoofed or modified emails from valid domains,describe how the Solution can support Participants to implement DMARC policy and verification, starting with implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standards.

3.9.6 Describe how the Solution can support Participants to block unnecessary file types attempting to enter the Enterprise's email gateway. Confirm that this will also support identifying unauthorized and unmanaged assets to remove or remediate.

3.9.7 Describe how the Solution can support Participants to deploy and maintain email server anti-malware protections, such as attachment scanning and/or sandboxing.

3.9.8 Describe how the Solution identifies potential Phishing campaigns and other email threats (i.e., artificial intelligence or other pattern recognition).

3.9.9 Describe how the Solution identifies and remediates Phishing attempts based on impersonation (e.g., a private email address that is similar to a known contact).

3.9.10 Describe how the Solution assists with efficient remediation of an attempted email threat (e.g., identification of potential victims, quarantine and removal of email, and other remediation strategies).

3.9.11 Describe how the proposed Solution is installed and integrated with Participant infrastructure (e.g., cloud-based architecture, gateway solution vs. API).

3.9.12 Describe how the proposed Solution supports end-to-end email encryption or equivalent data protection.

3.9.13 Describe any features of the Solution designed to detect and/or prevent unauthorized data exfiltration.

3.9.14 Describe how the Solution may simulate an email threat (impersonation, Phishing) to support user education.

3.9.15 Describe any additional features of the Solution that support email and web browser protections.

3.10 Malware Defenses

Proposed Solution(s): List all equipment, software, services and other products included in the Proposal that are offered in response to the requirements in this section. For each item or collection of items, add a Solution

Name and list the corresponding line number(s) from the Pricing Form. If you have provided additional technical literature or other reference materials for the Proposed Solution(s), include the page number(s) where the documentation can be found in the Proposal.

Examples of Proposed Solutions: For this section, Providers may consider proposing antimalware software, anti-exploitation policy management and tools, and other Solutions that meet the associated requirements. If the Provider proposal includes a Solution with multiple components, configuration options, or pricing tiers, the Solution may be listed on one line in the table below with the appropriate references to the line numbers corresponding to each of the options and components included on the pricing form (e.g., Proposed Solution - *Brand Name Malware Defense Software,* Line Number(s) - *5-25*).

Proposed Solution Name	Line Number(s) *From Pricing Form*	Page Number(s) *Reference Material*

3.10.0 Describe how the Solution can support Participants to prevent or control the installation, spread, and execution of malicious applications, code, or scripts on Enterprise assets.

3.10.1 Describe how the Solution can support Participants to deploy and maintain anti-malware software on all Enterprise assets.

3.10.2 Describe how the Solution can support Participants to configure automatic updates for anti-malware signature files on all Enterprise assets.

3.10.3 Describe how the Solution can support Participants to disable autorun and autoplay auto-execute functionality for removable media.

3.10.4 Describe how the Solution can support Participants to configure anti-malware software to automatically scan removable media.

3.10.5 Describe how the Solution can support Participants to enable anti-exploitation features on Enterprise assets and software.

3.10.6 Describe how the Solution can support Participants to centrally manage anti-malware software.

3.10.7 Describe how the Solution can support Participants to use behavior-based anti-malware software.

3.10.8 Please describe how the Solution supports the identification of any points of infection or origination of the malware attack.

3.10.9 Describe how the Solution identifies new threats and incorporates updates to the malware protection software and tools.

3.10.10 Describe how the Solution updates are propagated out to all Participant devices (including devices used remotely/off-network).

3.10.11 Confirm whether the Solution provides the flexibility to roll back to a previous version of the malware protection software if needed (e.g., a bug is identified that is preventing use of a legitimate, essential program).

3.10.12 Describe the communication and remediation workflow when a new threat has been identified (e.g., a previously unidentified Zero-Day Exploit).

3.10.13 Describe protections the Solution has in place to prevent disabling or modifying the malware defense program(s).

3.10.14 Describe any additional features of the Solution that support malware defenses.

3.11 Data Recovery Solutions

Proposed Solution(s): List all equipment, software, services and other products included in the Proposal that are offered in response to the requirements in this section. For each item or collection of items, add a Solution Name and list the corresponding line number(s) from the Pricing Form. If you have provided additional technical literature or other reference materials for the Proposed Solution(s), include the page number(s) where the documentation can be found in the Proposal.

Examples of Proposed Solutions: For this section, Providers may consider proposing backup solutions, ransomware protections, data recovery services, and other Solutions that meet the associated requirements. If the Provider proposal includes a Solution with multiple components, configuration options, or pricing tiers, the Solution may be listed on one line in the table below with the appropriate references to the line numbers corresponding to each of the options and components included on the pricing form (e.g., Proposed Solution - *Brand Name Hosted Backup and Recovery Storage and Services,* Line Number(s) - *5-25*)

Proposed Solution Name	Line Number(s) *From Pricing Form*	Page Number(s) *Reference Material*

**3.11.0 Describe how the Solution can support Participants to establish and maintain data recovery practices sufficient to restore in-scope Enterprise assets to a pre-incident and trusted state. **

3.11.1 Describe how the Solution can support Participants to establish and maintain a data recovery process. Please also describe how, in the process, Participants can address the scope of data recovery activities, recovery prioritization, and the security of backup data. Please also describe any tools that can support Participants to review and update documentation annually, or when significant Enterprise changes occur that could impact this Safeguard.

3.11.2 Describe how the Solution can support Participants to perform automated backups of in-scope Enterprise assets. Please also describe any tools that can support Participants to run backups weekly, or more frequently, based on the sensitivity of the data.

3.11.3 Describe how the Solution can support Participants to protect recovery data with equivalent controls to the original data. Reference encryption or data separation, based on requirements.

3.11.4 Describe how the Solution can support Participants to establish and maintain an isolated instance of recovery data. Example implementations include, version controlling backup destinations through offline, cloud, or off-site systems or services.

3.11.5 Describe how the Solution can support Participants to routinely and proactively test backup recovery for a sampling of in-scope Enterprise assets.

3.11.6 Describe any features within the Solution to protect and monitor backup copies from threats and unauthorized edits.

3.11.7 Describe any additional features of the Solution that support data backup and recovery.

3.12 Network Infrastructure Management

Proposed Solution(s): List all equipment, software, services and other products included in the Proposal that are offered in response to the requirements in this section. For each item or collection of items, add a Solution Name and list the corresponding line number(s) from the Pricing Form. If you have provided additional technical literature or other reference materials for the Proposed Solution(s), include the page number(s) where the documentation can be found in the Proposal.

Examples of Proposed Solutions: For this section, Providers may consider proposing secure network design services, network and infrastructure management, VPN solutions, network equipment, network documentation services, managed network equipment and services, and other Solutions that meet the associated requirements. For each technical Solution, please be clear about whether the Solution would be installed onsite or is a hosted solution. If the Provider proposal includes a Solution with multiple components, configuration options, or pricing tiers, the Solution may be listed on one line in the table below with the appropriate references to the line numbers corresponding to each of the options and components included on the pricing form (e.g., Proposed Solution - *Company Name Managed Network Services Options,* Line Number(s) - *5-25*)

Proposed Solution Name	Line Number(s) *From Pricing Form*	Page Number(s) *Reference Material*

3.12.0 Describe how the Solution can support Participants to establish, implement, and actively manage (track, report, correct) network devices, in order to prevent attackers from exploiting vulnerable network services and access points.

3.12.1 Describe how the Solution can support Participants to ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network-as-a-service (NaaS) offerings. Please also describe any tools that can support Participants to review software versions monthly, or more frequently, to verify software support.

3.12.2 Describe how the Solution can support Participants to establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.

3.12.3 Describe how the Solution can support Participants to securely manage network infrastructure. Example implementations include version-controlled-infrastructure-as-code, and the use of secure network protocols, such as SSH and HTTPS.

3.12.4 Describe how the Solution can support Participants to establish and maintain architecture diagram(s) and/or other network system documentation. Please also describe any tools that can support Participants to review and update documentation annually, or when significant Enterprise changes occur that could impact this Safeguard.

3.12.5 Describe how the Solution can support Participants to Centralize Network Authentication, Authorization, and Auditing (AAA).

3.12.6 Describe how the Solution can support Participants to use secure network management (e.g., Network Access Control) and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater).

3.12.7 Describe how the Solution can support Participants to require users to authenticate to Enterprise-managed VPN and authentication services prior to accessing Enterprise resources on end-user devices.

3.12.8 Describe how the Solution can support Participants to establish and maintain dedicated computing resources, either physically or logically separated, for all administrative tasks or tasks requiring administrative access. The computing resources should be segmented from the Enterprise's primary network and not be allowed internet access.

3.12.9 Describe how the Solution would provide support managing SSL certificates to implement a Public Key Infrastructure (PKI).

3.12.10 Describe how the Solution supports implementation of zero-trust design/security principles.

3.12.11 If the Solution offered includes full-service network management (e.g., contracting out implementation and maintenance of IT infrastructure), describe the full scope of services offered as a part of the Solution. Include detailed information to clearly identify what network management activities could/would be the responsibility of the Vendor and what would be the responsibility of the Participant.

3.12.12 Describe any additional features of the Solution that support network infrastructure management.

3.13 Network Monitoring and Defense

Proposed Solution(s): List all equipment, software, services and other products included in the Proposal that are offered in response to the requirements in this section. For each item or collection of items, add a Solution Name and list the corresponding line number(s) from the Pricing Form. If you have provided additional technical literature or other reference materials for the Proposed Solution(s), include the page number(s) where the documentation can be found in the Proposal.

Examples of Proposed Solutions: For this section, Providers may consider proposing network intrusion detection solutions, intrusion prevention solutions, network filtering and segmentation tools, access control, security event logging and alerting tools, and other Solutions that meet the associated requirements. If the Provider proposal includes a Solution with multiple components, configuration options, or pricing tiers, the Solution may be listed on one line in the table below with the appropriate references to the line numbers corresponding to each of the options and components included on the pricing form (e.g., Proposed Solution - *Brand Name Intrusion Detection Solution and Configuration Options,* Line Number(s) - *5-25*)

Proposed Solution Name	Line Number(s) *From Pricing Form*	Page Number(s) *Reference Material*

**3.13.0 Describe how the Solution can support Participants to operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the Enterprise's network infrastructure and user base. **

3.13.1 Describe how the Solution can support Participants to centralize security event alerting across Enterprise assets for log correlation and analysis. Best practice implementation requires the use of a SIEM, which includes vendor-defined event correlation alerts. A log analytics platform configured with security-relevant correlation alerts also satisfies this Safeguard.

3.13.2 Describe how the Solution can support Participants to deploy a host-based intrusion detection solution on Enterprise assets, where appropriate and/or supported.

3.13.3 Describe how the Solution can support Participants to deploy a network intrusion detection solution on Enterprise assets, where appropriate. Example implementations include the use of a Network Intrusion Detection System (NIDS) or equivalent cloud service provider (CSP) service.

3.13.4 Describe how the Solution can support Participants to perform traffic filtering between network segments, where appropriate.

3.13.5 Describe how the Solution can support Participants to manage access control for assets remotely connecting to Enterprise resources. Please also describe tools that can support Participants to determine amount of access to Enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the Enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.

3.13.6 Describe how the Solution can support Participants to collect network traffic flow logs and/or network traffic to review and alert upon from network devices.

3.13.7 Describe how the Solution can support Participants to deploy a host-based intrusion prevention solution on Enterprise assets, where appropriate and/or supported. Example implementations include use of an Endpoint Detection and Response (EDR) client or host-based IPS agent.

3.13.8 Describe how the Solution can support Participants to deploy a network intrusion prevention solution, where appropriate. Example implementations include the use of a Network Intrusion Prevention System (NIPS) or equivalent CSP service.

3.13.9 Describe how the Solution can support Participants to deploy port-level access control. Confirm that port-level access control utilizes 802.1x, or similar network access control protocols, such as certificates, and may incorporate user and/or device authentication.

3.13.10 Describe how the Solution can support Participants to perform application layer filtering. Example implementations include a filtering proxy, application layer firewall, or gateway.

3.13.11 Describe how the Solution can support Participants to tune security event alerting thresholds monthly, or more frequently.

3.13.12 Describe automated features within the Solution designed to remediate threats without direct intervention by Participant staff.

3.13.14 Describe any additional features of the Solution that support network monitoring and defense.

3.14 Security Awareness and Skills Training

Proposed Solution(s): List all equipment, software, services and other products included in the Proposal that are offered in response to the requirements in this section. For each item or collection of items, add a Solution Name and list the corresponding line number(s) from the Pricing Form. If you have provided additional technical literature or other reference materials for the Proposed Solution(s), include the page number(s) where the documentation can be found in the Proposal.

Examples of Proposed Solutions: For this section, Providers may consider proposing on-demand or instructor-led training, virtual learning tools, security curriculum for students and staff, simulation tools (e.g., phishing campaigns), and other Solutions that meet the associated requirements. If the Provider proposal includes a Solution with multiple components, configuration options, or pricing tiers, the Solution may be listed on one line in the table below with the appropriate references to the line numbers corresponding to each of the options and components included on the pricing form (e.g., Proposed Solution - *Cybersecurity On-Demand Training for non-IT Staff,* Line Number(s) - *5-25*)

Proposed Solution Name	Line Number(s) *From Pricing Form*	Page Number(s) *Reference Material*

**3.14.0 Describe how the Solution can support Participants to establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the Enterprise. **

3.14.1 Describe how the Solution can support Participants to establish and maintain a security awareness program. The purpose of a security awareness program is to educate the Enterprise’s workforce on how to interact with Enterprise assets and data in a secure manner. Please also describe any tools that can support Participants to conduct training at hire and, at a minimum, annually. Please describe any tools that can support Participants to review and update content annually, or when significant Enterprise changes occur that could impact this Safeguard.

3.14.2 Describe how the Solution can support Participants to train workforce members to recognize social engineering attacks, such as phishing, pre-texting, and tailgating.

3.14.3 Describe how the Solution can support Participants to train workforce members on authentication best practices. Example topics include MFA, password composition, and credential management.

3.14.4 Describe how the Solution can support Participants to train workforce members on how to identify and properly store, transfer, archive, and destroy sensitive data. This also includes training workforce members on clear screen and desk best practices, such as locking their screen when they step away from their Enterprise asset, erasing physical and virtual whiteboards at the end of meetings, and storing data and assets securely.

3.14.5 Describe how the Solution can support Participants to train workforce members to be aware of causes for unintentional data exposure. Example topics include mis-delivery of sensitive data, losing a portable end-user device, or publishing data to unintended audiences.

3.14.6 Describe how the Solution can support Participants to train workforce members to be able to recognize a potential incident and be able to report such an incident.

3.14.7 Describe how the Solution can support Participants to train workforce to understand how to verify and report out-of-date software patches or any failures in automated processes and tools. Part of this training should include notifying IT personnel of any failures in automated processes and tools.

3.14.8 Describe how the Solution can support Participants to train workforce members on the dangers of connecting to, and transmitting data over, insecure networks for Enterprise activities. Please also describe tools to support if the Enterprise has remote workers, training that must include guidance to ensure that all users securely configure their home network infrastructure.

3.14.9 Describe how the Solution can support Participants to conduct role-specific security awareness and skills training. Example implementations include secure system administration courses for IT professionals, vulnerability awareness and prevention training for web application developers, and advanced social engineering awareness training for high-profile roles.

3.14.10 Describe any features in the Solution designed to assign, monitor completion of, and report on training participation.

3.14.11 Describe the format and delivery of available training (e.g., training manuals, videos, interactive assignments) and how the training is tailored to the appropriate audience.

3.14.12 Confirm whether the Solution offers trainings that are age-appropriate for K-12 students and parents.

3.14.12.1 Confirm whether student and parent materials are available in languages other than English. List all translated materials and the languages available.

3.14.13 Provide sample training materials to demonstrate the scope, content and formatting of available trainings.

3.14.14 Describe any additional features of the Solution that support security awareness and skills training.

3.15 Service Provider Management

Proposed Solution(s): List all equipment, software, services and other products included in the Proposal that are offered in response to the requirements in this section. For each item or collection of items, add a Solution Name and list the corresponding line number(s) from the Pricing Form. If you have provided additional technical literature or other reference materials for the Proposed Solution(s), include the page number(s) where the documentation can be found in the Proposal.

Examples of Proposed Solutions: For this section, Providers may consider proposing contract and contact management solutions, security agreement templates, compliance monitoring services, identity and workflow management solutions (for service provider access) and other Solutions that meet the associated requirements. If the Provider proposal includes a Solution with multiple components, configuration options, or pricing tiers, the Solution may be listed on one line in the table below with the appropriate references to the line numbers corresponding to each of the options and components included on the pricing form (e.g., Proposed Solution - *Identity Management Solution (with service provider workflows),* Line Number(s) - *5-25*)

Proposed Solution Name	Line Number(s) *From Pricing Form*	Page Number(s) *Reference Material*

**3.15.0 Describe how the Solution can support Participants to develop a process to evaluate service providers who hold sensitive data, or are responsible for an Enterprise's critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately. **

3.15.1 Describe how the Solution can support Participants to establish and maintain an inventory of service providers. Describe how the Solution ensures that the inventory is to list all known service providers, include classification(s), and designate an Enterprise contact for each service provider. Please also describe any tools that can support Participants to review and update the inventory annually, or when significant Enterprise changes occur that could impact this Safeguard.

3.15.2 Describe how the Solution can support Participants to establish and maintain a service provider management policy. Ensure the policy addresses the classification, inventory, assessment, monitoring, and decommissioning of service providers. Please also describe any tools that can support Participants to review and update the policy annually, or when significant Enterprise changes occur that could impact this Safeguard.

3.15.3 Describe how the Solution can support Participants to classify service providers. Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk. Please also describe any tools that can support Participants to update and review classifications annually, or when significant Enterprise changes occur that could impact this Safeguard.

3.15.4 Describe how the Solution can support Participants to ensure service provider contracts include security requirements. Example requirements may include minimum security program requirements, security incident and/or data breach notification and response, data encryption requirements, and data disposal commitments. These security requirements must be consistent with the Enterprise's service provider management policy. Please also describe any tools that can support Participants to review service provider contracts annually to ensure contracts are not missing security requirements.

3.15.5 Describe how the Solution can support Participants to assess service providers consistent with the Enterprise's service provider management policy. Assessment scope may vary based on classification(s), and may include review of standardized assessment reports, such as Service Organization Control 2 (SOC 2) and Payment Card Industry (PCI) Attestation of Compliance (AoC), customized questionnaires, or other appropriately rigorous processes. Please also describe any tools that can support Participants to reassess service providers annually, at a minimum, or with new and renewed contracts.

3.15.6 Describe how the Solution can support Participants to monitor service providers consistent with the Enterprise's service provider management policy. Monitoring may include periodic reassessment of service provider compliance, monitoring service provider release notes, and dark web monitoring.

3.15.7 Describe how the Solution can support Participants to securely decommission service providers. Example considerations include user and service account deactivation, termination of data flows, and secure disposal of Enterprise data within service provider systems.

3.15.8 Describe any provider-agnostic badging, certification or other evaluation programs supported by the Solution. Describe how providers are evaluated, including any requirements for certification renewal.

3.15.9 Describe any additional features of the Solution that support service provider management.

3.16 Application Software Security

Proposed Solution(s): List all equipment, software, services and other products included in the Proposal that are offered in response to the requirements in this section. For each item or collection of items, add a Solution Name and list the corresponding line number(s) from the Pricing Form. If you have provided additional technical literature or other reference materials for the Proposed Solution(s), include the page number(s) where the documentation can be found in the Proposal.

Examples of Proposed Solutions: For this section, Providers may consider proposing systems for detection of application vulnerabilities, platforms and services to support secure application development, monitoring and testing of applications and application infrastructure, and other Solutions that meet the associated requirements. If the Provider proposal includes a Solution with multiple components, configuration options, or pricing tiers, the Solution may be listed on one line in the table below with the appropriate references to the line numbers corresponding to each of the options and components included on the pricing form (e.g., Proposed Solution - *Application Penetration Testing Services,* Line Number(s) - *5-25*)

Proposed Solution Name	Line Number(s) *From Pricing Form*	Page Number(s) *Reference Material*

3.16.0 Describe how the Solution can support Participants to manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they can impact the Enterprise.

3.16.1 Describe how the Solution can support Participants to establish and maintain a secure application development process.

3.16.1.1 (a.)Describe how the Solution can support Participants to establish and maintain a secure application development process.

(b.)Describe how the Proposed Solution enhances application security with design standards, coding practices, developer training, vulnerability management, third-party code management, and/or application testing procedures.

(a.)
(b.)

3.16.2 Describe how the Solution can support Participants to establish and maintain a process to accept and address reports of software vulnerabilities, including providing a means for external entities to report. The process may include such items as: a vulnerability handling policy that identifies reporting process, responsible party for handling vulnerability reports, and a process for intake, assignment, remediation, and remediation testing. Describe how, as part of the process, Participants can use a vulnerability tracking system that includes severity ratings, and metrics for measuring timing for identification, analysis, and remediation of vulnerabilities.

3.16.3 Describe how the Solution can support Participants to identify security vulnerabilities and perform root cause analysis..

3.16.4 Describe how the Solution can support Participants to establish and manage an updated inventory of third-party components used in development as well as components slated for future use. This inventory should include any risks that each third-party component could pose. Please also describe how the Solution supports monitoring these components to identify any changes or updates, and validate that the components are still supported.

3.16.5 Describe how the Solution can support Participants to use up-to-date and trusted third-party software components. Describe how, when possible, the Solution can support Participants to choose established and proven frameworks and libraries that provide adequate security. Please also describe tools that can support Participants to acquire these components from trusted sources or evaluate the software for vulnerabilities before use.

3.16.6 Describe how the Solution can support Participants to establish and maintain a severity rating system and process for application vulnerabilities that facilitates prioritizing the order in which discovered vulnerabilities are fixed. Describe how this process includes setting a minimum level of security acceptability for releasing code or applications.

3.16.7 Describe how the Solution can support Participants to use standard, industry-recommended hardening configuration templates for application infrastructure components. This includes underlying servers, databases, and web servers, and applies to cloud containers, Platform as a Service (PaaS) components, and SaaS components.

3.16.8 Describe how the Solution can support Participants to maintain separate environments for production and non-production systems.

3.16.9 Describe how the Solution can provide Participants’ software development personnel training in writing secure applications for their specific development environment and responsibilities. Training can include general security principles and application security standard practices.

3.16.10 Describe how the Solution can support Participants to apply secure design principles in application architectures. Secure design principles include the concept of least privilege and enforcing mediation to validate every operation that the user makes, promoting the concept of "never trust user input." Examples include ensuring that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats.

3.16.11 Describe how the Solution can support Participants to leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging.

3.16.12 Describe how the Solution can support Participants to analyze applications and Participant development processes to verify that secure application development practices are being followed.

3.16.13 Describe how the Solution supports application penetration testing.

3.16.14 Describe how the Solution can support Participants to conduct threat modeling to identify and address application security design flaws.

3.16.15 Describe any additional features of the Solution that support application software security.

3.17 Incident Response Management

Proposed Solution(s): List all equipment, software, services and other products included in the Proposal that are offered in response to the requirements in this section. For each item or collection of items, add a Solution Name and list the corresponding line number(s) from the Pricing Form. If you have provided additional technical literature or other reference materials for the Proposed Solution(s), include the page number(s) where the documentation can be found in the Proposal.

Examples of Proposed Solutions: For this section, Providers may consider proposing incident response assessments and templates, incident response as a service, facilitation of incident response exercises, incident monitoring, training, and other Solutions that meet the associated requirements. If the Provider proposal includes a Solution with multiple components, configuration options, or pricing tiers, the Solution may be listed on one line in the table below with the appropriate references to the line numbers corresponding to each of the options and components included on the pricing form (e.g., Proposed Solution - *Incident Response Assessment and Process Development Services,* Line Number(s) - *5-25*)

Proposed Solution Name	Line Number(s) *From Pricing Form*	Page Number(s) *Reference Material*

**3.17.0 Describe how the Solution can support Participants to establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack. **

3.17.1 Describe how the Solution can support Participants to designate and document individuals who have responsibility for managing the Enterprise's incident handling process. The Solution should identify primary and backup personnel that are responsible for the coordination and documentation of incident response and recovery efforts and can consist of employees internal to the Enterprise, third-party vendors, or a hybrid approach.

3.17.2 Describe how the Solution can support Participants to establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, third-party vendors, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders. Please also describe tools that can support Participants to verify contacts annually to ensure that information is up-to-date.

3.17.3 Describe how the Solution can support Participants to establish and maintain an Enterprise process for the workforce to report security incidents. Confirm that the process includes reporting timeframe, personnel to report to, mechanism for reporting, and the minimum information to be reported. Ensure the process is publicly available to all of the workforce.

3.17.4 Describe how the Solution can support Participants to establish and maintain an incident response process that addresses roles and responsibilities, compliance requirements, and a communication plan.

3.17.5 Describe how the Solution can support Participants to assign key roles and responsibilities for incident response, including staff from legal, IT, information security, facilities, public relations, human resources, incident responders, and analysts, as applicable.

3.17.6 Describe how the Solution can support Participants to determine which primary and secondary mechanisms will be used to communicate and report during a security incident. Mechanisms can include phone calls, emails, or letters. Keep in mind that certain mechanisms, such as emails, can be affected during a security incident.

3.17.7 Describe how the Solution can support Participants to plan and conduct routine incident response exercises and scenarios for key personnel involved in the incident response process to prepare for responding to real-world incidents. Exercises need to test communication channels, decision making, and workflows. Please also describe tools that can support Participants to conduct testing on an annual basis, at a minimum.

3.17.8 Describe how the Solution can support Participants to conduct post-incident reviews. Post-incident reviews help prevent incident recurrence through identifying lessons learned and follow-up action.

3.17.9 Describe how the Solution can support Participants to establish and maintain security incident thresholds, including, at a minimum, differentiating between an incident and an event. Examples can include: abnormal activity, security vulnerability, security weakness, data breach, privacy incident, etc.

3.17.10 Describe any services offered by Vendor to manage Participant’s incident response (e.g., Provider will conduct investigation, draft incident reports, recommend remediation steps). Please include details about the scope (and limitations) of Vendor’s investigations in response to an incident (e.g., network intrusion, data exfiltration, user account compromise, malware/compromised devices).

3.17.11 Describe services and tools available through the Solution to support Participants in implementing remediation or mitigation strategies in response to an incident.

3.17.12 Describe the framework(s) utilized by the Vendor for incident response and management (e.g., NIST, MITRE).

3.17.13 Describe any additional features of the Solution that support incident response management.

3.18 Penetration Testing

Proposed Solution(s): List all equipment, software, services and other products included in the Proposal that are offered in response to the requirements in this section. For each item or collection of items, add a Solution Name and list the corresponding line number(s) from the Pricing Form. If you have provided additional technical literature or other reference materials for the Proposed Solution(s), include the page number(s) where the documentation can be found in the Proposal.

Examples of Proposed Solutions: For this section, Providers may consider proposing penetration testing and remediation platforms and services, and other Solutions that meet the associated requirements. If the Provider proposal includes a Solution with multiple components, configuration options, or pricing tiers, the Solution may be listed on one line in the table below with the appropriate references to the line numbers corresponding to each of the options and components included on the pricing form (e.g., Proposed Solution - *Brand Name Pen Test Tool and Support Options,* Line Number(s) - *5-25*)

Proposed Solution Name	Line Number(s) *From Pricing Form*	Page Number(s) *Reference Material*

**3.18.0 Describe how the Solution can support Participants to test the effectiveness and resiliency of Enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker. **

3.18.1 Describe how the Solution can support Participants to establish and maintain a penetration testing program appropriate to the size, complexity, and maturity of the Enterprise. Please describe penetration testing program characteristics including scope, such as: network, web application, Application Programming Interface (API), hosted services, and physical premise controls; frequency; limitations, such as acceptable hours, and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements.

3.18.2 Describe how the Solution can support Participants to perform periodic external penetration tests based on program requirements, no less than annually. External penetration testing must include Enterprise and environmental reconnaissance to detect exploitable information. Describe if the testing is clear box or opaque box.

3.18.3 Describe how the Solution can support Participants to remediate penetration test findings based on the Enterprise's policy for remediation scope and prioritization.

3.18.4 Describe how the Solution can support Participants to validate security measures after each penetration test. If deemed necessary, describe tools that can support Participants to modify rulesets and capabilities to detect the techniques used during testing.

3.18.5 Describe how the Solution can support Participants to perform periodic internal penetration tests based on program requirements, no less than annually.

3.18.6 Describe the penetration testing and reporting tools proposed in the Solution.

3.18.7 Describe the scope of penetration testing provided in the Solution. Provide details about the level of testing performed (e.g., passive network scanning, or active assessment/attempted intrusion) and the techniques used. Include supporting documentation about the qualifications and expertise of the staff performing the penetration testing.

3.18.8 Provide samples of reports and other artifacts that demonstrate the scope of available penetration testing and actionable information that would be provided to Participant.

3.18.9 Describe who performs the penetration testing, including if penetration testing is performed by Vendor's employees or a third party/subcontractor.

3.18.10 Describe Vendor's security practices and confidentiality policies for penetration test results and recommended remediation steps.

3.18.11 Describe any additional features of the Solution that support penetration testing.

3.19 Security Services

Proposed Solution(s): List all equipment, software, services and other products included in the Proposal that are offered in response to the requirements in this section. For each item or collection of items, add a Solution Name and list the corresponding line number(s) from the Pricing Form. If you have provided additional technical literature or other reference materials for the Proposed Solution(s), include the page number(s) where the documentation can be found in the Proposal.

Examples of Proposed Solutions: For this section, Providers may consider proposing professional services, resources, templates, training and other Solutions that meet the associated requirements. If the Provider proposal includes a Solution with multiple components, configuration options, or pricing tiers, the Solution may be listed on one line in the table below with the appropriate references to the line numbers corresponding to each of the options and components included on the pricing form (e.g., Proposed Solution - *Security Operations Center (as a service, with defined support level options),* Line Number(s) - *5-25*)

Proposed Solution Name	Line Number(s) *From Pricing Form*	Page Number(s) *Reference Material*

**3.19.0 Describe the scope of professional services related to security and IT administration available from the Vendor. **

**3.19.1 ** Provide a summary of Vendor's consulting personnel and consulting partnerships. Include details about the company and typical project team organizational structure, qualifications of proposed consultants and any other relevant supporting documentation to demonstrate the level of expertise of company personnel.

3.19.2 Describe the Vendor's typical approach to a consulting/professional services partnership. Include a sample statement of work and/or project scope.

3.19.3 Confirm whether Vendor Security-as-a-Service (e.g., will manage network infrastructure and security on behalf of Participant). If Vendor offers comprehensive security and/or network management services, please describe the scope and fee structure for those services.

3.19.4 Describe any additional offerings related to Security Services.

3.20 Campus Safety (Facility Security)

Proposed Solution(s): List all equipment, software, services and other products included in the Proposal that are offered in response to the requirements in this section. For each item or collection of items, add a Solution Name and list the corresponding line number(s) from the Pricing Form. If you have provided additional technical literature or other reference materials for the Proposed Solution(s), include the page number(s) where the documentation can be found in the Proposal.

Examples of Proposed Solutions: For this section, Providers may consider proposing professional services, equipment, installation services, supplies, software platforms and other items that support keeping school campuses and other Participant facilities safe. Examples may include video surveillance equipment and systems, emergency alerting and response systems, electronic locks, and visitor/volunteer management platforms. If the Provider proposal includes a Solution with multiple components, configuration options, or pricing tiers, the Solution may be listed on one line in the table below with the appropriate references to the line numbers corresponding to each of the options and components included on the pricing form (e.g., Proposed Solution - *Security Operations Center (as a service, with defined support level options),* Line Number(s) - *5-25*)

Proposed Solution Name	Line Number(s) *From Pricing Form*	Page Number(s) *Reference Material*

**3.20.0 Describe the Vendor's proposed Solution(s) and how they contribute to safe and secure school campuses and/or public facilities. **

3.20.1 Provide an overview of Vendor's support for installation and/or implementation of the proposed Solution(s). Include descriptions of manufacturer-issued or other certifications as applicable to the installation of the proposed products.

Visitor and Volunteer Management

3.20.2 Describe how the Solution supports secure and efficient check-in of visitors and volunteers at Participant campuses/facilities.

3.20.3 Describe options available for the creation/printing of personalized visitor and volunteer badges at the time of check in.

3.20.4 Describe how the Solution supports scanning of government-issued identification for a more secure, validated check-in process. List all ID types (e.g., drivers' license, passport card, passport book) supported by the Solution and equipment options.

3.20.5 Describe the capabilities of the Solution to support real-time checks of visitors and volunteers against national sex offender registries and any other similar data sources.

3.20.6 Describe how the Solution supports more extensive background checks where needed (e.g., criminal background check through the Department of Justice for an adult that may accompany a class on an overnight field trip).

3.20.7 Provide an overview of the check-in and check-out process from the perspective of the visitor or volunteer (include screenshots of the process).

3.20.8 Confirm whether the Solution supports identifying potential visitors that should have limited or no access to Participant facilities ("flagged contacts"). Example: a parent/guardian whose access to campus is restricted by court order.

3.20.9 Describe how the Solution alerts appropriate staff to a potential security issue (e.g., potential sex offender or flagged contact on campus). Provide details on configuration related to how alerts are displayed in the system, who may be notified, and how the desired workflow can be differentiated by the type of alert or facility where the alert was generated.

3.20.10 Provide examples of reporting tools available in the Solution. Minimally, reports should include daily logs of visitors and volunteers on campus and any reported alerts.

3.20.11 Confirm whether the Solution offers a customizable volunteer application to collect volunteer contact information, interests in specific activities, and agreement to Participant volunteer policies and procedures (e.g., electronic acknowledgement of volunteer policy).

3.20.12 Describe any features available in the Solution to solicit and manage volunteers for a specific event and/or activity. Include screenshots where possible to illustrate the process.

3.20.13 Describe any additional offerings related to Volunteer and Visitor Management.

Student Attendance Support

3.20.14 Provide an overview of how the Solution supports tracking student attendance and/or whereabouts on campus to promote student safety.

3.20.15 Describe how the Solution may integrate with the Participant's Student Information System (SIS) to pull student data to support these attendance features and push desired attendance data back to the SIS.

3.20.16 Describe features available in the Solution to support tracking students' late arrival to campus. Example: A Solution that students or staff may use to generate an automated tardy slip with the time/date of the late arrival for students to present to their teacher, and corresponding summary reports of student tardies.

3.20.17 Describe features available in the Solution to support students' early dismissal (e.g., leaving campus midday for a doctor's appointment). Describe how the Solution promotes safe release of the student (e.g., verifying the individual picking up the student is an authorized contact).

3.20.18 Describe how the Solution supports tracking student attendance in flexible periods during the day (e.g., a tutorial or advisement section where students do not have a pre-assigned room number).

3.20.19 Confirm the Solution allows for students to register for or select a teacher or classroom destination for a flexible period.

3.20.20 Confirm the Solution allows school staff to pre-designate or assign students' destination for a flexible period. Provide screenshots to illustrate how staff may assign destinations to individual and groups of students.

3.20.21 Describe how the Solution supports confirming attendance during flexible periods.

3.20.22 Describe and provide examples of reports and management features available in the system to identify students that have not signed up for a flexible period destination or students who signed up for, but did not attend their assigned destination.

3.20.23 Describe any additional offerings related to tracking student attendance and location.

Other Campus Safety (Facility Enhancements)

3.20.24 Describe Vendor offerings and equipment options related to the security of Participant Facilities. Offerings may include video surveillance, motion detectors/lights, intrusion sensors, electronic locks, public address systems, alarms, emergency alert/lockdown systems or any other Solution(s) designed to protect Participant facilities and personnel. Note: Vendors may provide a brief narrative response to this requirement here and attach detailed specification sheets and product lists for Solution(s) with a variety of component options (e.g., surveillance cameras). If additional specification sheets are attached, indicate the page numbers corresponding to their location in the Proposal document.

3.20.25 Describe Vendor Solution(s) to support active monitoring and management of campus/facility safety. For example, for a video surveillance program, describe distinguishing features of the platform that allow participants to identify, respond to and investigate potential security incidents. For lockdown solutions, describe features that allow for an immediate lockdown and communication with essential Participant staff and/or first responders.

3.20.26 Describe Vendor professional services available to support the installation, monitoring and/or maintenance of equipment, software and other Solution(s) related to campus/facility security. For remote support, include support hours. For installation services, include information about any limitations to areas served by the Vendor and/or Vendor subcontractors.

3.20.27 Describe any additional offerings related to Campus Safety or Facility Security.

IT Administration

4.1 Help Desk

Module	Included in Proposal (Y/N)	Individually Licensed (Y/N)	Package Only (Y/N)	Comments (Please list applications that must be bundled with purchase if applicable)
4.1.1 Ticketing and Support Workflows				
4.1.2 Knowledgebase				

Key

Section 3 RFP Term	**Meaning**
End-User or Requestor	Individual(s) who will request services via the Solution, such as a teacher who submits a ticket requesting assistance with a computer problem.
Technician	Individual(s) who will respond to service requests, such as Information Technology staff member(s) who receive and respond to tickets.
System Administrator	Individual(s) who are involved in designing the structure of the Solution.
Workgroup	Multiple members with similar roles who respond to a shared group of tickets, such as the networking team and programming team.

4.1.1 Ticketing and Support Workflows

For each requirement in the table below, please indicate “Yes” the requirement is met in the current version of the solution, “No” the requirement is not met by the Solution, or “P” if the requirement will be met in a future, planned release of the Solution. If the requirement will be met in a future release, please provide the current status of the feature (e.g., in development, in testing) and the planned release date.

	Yes	No	P	Comments
**4.1.1.1 Confirm that the Solution offers an accessible web interface for quickly creating support tickets. **				
4.1.1.2 Confirm that the Solution supports efficient assignment and updating of tickets.				
4.1.1.3 Confirm that the Solution supports automated communications related to ticket updates and status.				
4.1.1.4 If the Solution provides email notifications related to ticket updates, confirm that email responses to the notifications will be appended to the ticket in the system.				
4.1.1.5 Confirm that tickets can be assigned to either an individual Technician or a Workgroup (Ticket Pool).				
4.1.1.6 Confirm that the Solution allows for custom branding (use of the Participant’s logo).				

4.1.1.7 Describe how End-Users may submit tickets. Examples may include: online/web-form, email, online chat, embedded web widget, phone system integration, or other tools.

**4.1.1.8 Describe the options available for end-users and technicians to access the system for current and past tickets (e.g., website, email, chat, IOS app, Android app, automated phone service).

4.1.1.9 Describe the security roles available in the system for technical support staff. Identify how access to tickets can be determined by end-user/requestor work location, technician work groups, ticket assignee, or other ticket attributes.

**4.1.1.10 Provide a brief description of the typical ticket workflow within the Solution. Include a description of how tickets are managed from initial submission, assignment, update, to closure/resolution. **

4.1.1.11 Identify the default ticket statuses provided in the Solution. Describe any automated processes or calculations (e.g., Service Level Agreements) based on the default statuses that come natively in the Solution.

4.1.1.12 Describe how the Solution supports differentiating workflows and/or settings based on Workgroups (e.g., Facilities, IT - Networking, IT- Programming).

**4.1.1.13 Describe how the Solution supports communication with End-Users about the status of their request/ticket. Please explain the degree to which notifications can be automated and customized by the Participant's organization. **

4.1.1.14 Describe how the Solution supports communication between Technicians that can be kept private from the end-user.

4.1.1.15 Define the extent to which ticket submission and/or routing forms are customizable.

4.1.1.16 Provide a screenshot of a standard ticket form.

4.1.1.17 Describe how the Solution supports shared Ticket Pools (tickets assigned to group rather than individual technician).

**4.1.1.18 Describe how End-Users, Technicians, and System Administrators can search for tickets. Clarify whether the system can locate a ticket by ticket number, key word, or other attributes. **

**4.1.1.19 Describe features available to save searches (create views) of tickets that share a common attribute (e.g., assigned technician, workgroup, status, date created/updated). **

4.1.1.20 Describe how the Solution supports granular categorization of tickets to support accurate and comprehensive search results. Examples may include automated/manual ticket tagging, custom fields for categorization, and other advanced search options.

4.1.1.21 Describe options available in the Solution to link related tickets. For example, if the organization is experiencing a site-wide outage, is it possible to connect all tickets related to the same event?

4.1.1.22 Describe how the Solution supports monitoring of ticket resolution timelines, Technician work time, and End-User wait times. Identify what data is available in the system to monitor ticket timelines.

**4.1.1.23 Describe the process for closing or resolving a ticket. Identify any automated processes that are or can be triggered as part of the ticket resolution process (e.g., satisfaction surveys). **

For each requirement in the table below, please indicate “Yes” the requirement is met in the current version of the solution, “No” the requirement is not met by the Solution, or “P” if the requirement will be met in a future, planned release of the Solution. If the requirement will be met in a future release, please provide the current status of the feature (e.g., in development, in testing) and the planned release date.

	Yes	No	P	Comments
4.1.1.24 Confirm that the Solution offers workflow tools to automate initial assignment of tickets.				
4.1.1.25 Confirm that ticket assignment can be automated by each of the following ticket attributes:				
a. Ticket Requestor work location.				
b. Custom drop-down fields (e.g., category, issue type) on the ticket form.				
c. Email address the ticket was sent to (e.g., ithelpdesk@agency.org vs. mnohelpdesk@agency.org) .				
d. Key words/text match within the submitted ticket based on assignments created by customer.				

4.1.1.26 Confirm that the Solution offers tools to automate the escalation of tickets based on the following attributes or events:				
a. The ticket is submitted as high-priority or the assigned Technician designates the ticket as high-priority.				
b. A specific amount of time has elapsed since a ticket event/change.				
c. Designated keywords (e.g. “urgent,” “emergency,” “outage”) are used in ticket description.				
4.1.1.27 Confirm that the Solution offers tools to automate or increase efficiency of responses to common, similar or related tickets.				

4.1.1.28 Describe workflows/tools available in the Solution to automate *assignment* of tickets to the appropriate Technician. Be specific about what user or ticket attributes can be used to automate ticket assignment.

4.1.1.29 Describe workflow/tools available in the Solution to automate *escalation* of tickets to a designated point of contact or supervisor. Describe features available to automate notification and/or reassignment of a ticket based on priority or elapsed time since the ticket was opened or updated.

4.1.1.30 Confirm whether the Solution allows the Participant to define Service Level Agreement (SLA) targets. Be specific about whether SLA targets are defined globally (one per Participant), or if they can be defined by Department, Workgroup or other category.

4.1.1.31 Describe tools available in the Solution to create efficiencies in responding to common, similar or related tickets. Examples may include: self-service resolution tools, automated response/artificial intelligence, tools to link tickets for mass updates on a related issue, ability to create canned responses for common tickets, or the ability to incorporate tutorials into the ticket response.

4.1.1.32 Describe how the Solution supports even distribution of work between Technicians, Workgroups, or groups of technicians/resources (ie: are tickets assigned randomly to users in a group, via a round robin approach within the group, is this customizable, etc.?).

4.1.1.33 Describe how the system can be used to create approval workflows for tickets when needed (e.g., budgetary approval for tickets that require facilities modification).

4.1.1.34 Describe reporting tools available in the Solution and provide sample reports.

4.1.1.35 Describe available integration with communication and/or project management platforms (e.g., Office 365, Google Workspace, Slack, Asana, SmartSheets, Jira).

4.1.1.36 Describe how the Solution supports invoicing and/or chargebacks (e.g., cost to fulfill a maintenance painting work order, cost of replacement equipment).

4.1.1.37 Describe available integrations with Inventory Solutions. If Vendor offers a fully integrated Inventory Solution, describe the core features of the Solution.

4.1.1.38 Describe any additional features offered by the Solution that assist with ticketing and support workflows. If there is any additional cost please be sure to describe it here and in the Pricing Form.

4.1.2 Knowledgebase

For each requirement in the table below, please indicate “Yes” the requirement is met in the current version of the solution, “No” the requirement is not met by the Solution, or “P” if the requirement will be met in a future, planned release of the Solution. If the requirement will be met in a future release, please provide the current status of the feature (e.g., in development, in testing) and the planned release date.

	Yes	No	P	Comments

4.1.2.1 Confirm that tutorials and/or articles (“Articles”) can be incorporated into the Solution as a user-interactive website (not just a repository of links).				
**4.1.2.2 Confirm that the knowledgebase is searchable by End-Users. Confirm that the search will look at the body of the article and other attributes of the article (e.g., title, author). **				
4.1.2.3 Confirm that the Solution allows access to and visibility of Articles to be restricted based on User Role (e.g., public, staff only, technician only).				
4.1.2.4 Confirm that the Solution shows viewing usage for each Article.				
4.1.2.5 Confirm that the Solution allows for End User rating of and/or commenting on Articles.				
4.1.2.6 Confirm that the created date and last updated date of each Article is visible to System Administrators and available in reports to help identify and maintain potentially outdated Articles.				

4.1.2.7 Describe how Articles can be categorized and what capabilities this allows.

4.1.2.8 Describe how Articles are linked in the ticketing Solution and how they can be shared with End Users (ie: via email, etc.).

4.1.2.9 Describe how access to and visibility of Articles can be restricted by User Role and any limitations on the number of permission groups.

4.1.2.10 Describe how internal users would log on to access Articles for internal users.

4.1.2.11 Describe how the Knowledgebase interacts with the ticketing components of the Solution. Show how an Article can be added by a Technician in a response to a ticket. Describe features in the Solution designed to automate/proactively identify appropriate Knowledgebase articles related to an open ticket (for End-Users and/or Technicians).

4.1.2.12 Describe features available to automatically identify and provide relevant Articles to End-Users during the Ticket creation process to support self-service resolution.

4.1.2.13 Clarify whether the Solution automatically prompts the End User to open a ticket (opens a ticket window) if a Knowledgebase search does not generate results.

4.1.2.14 Describe how Articles may be promoted or featured as needed. For example, Articles relevant to year-end procedures could be made more visible during the appropriate time of the year.

4.1.2.15 Describe the Article creation and editing experience for knowledgebase System Administrators and authors. What capabilities and features are present in the editor (markup languages, embedded videos, etc)?

4.1.2.16 Describe content management tools available for life-cylcle management of Articles, including: solutions for identifying and updating stale/outdated articles, versioning capabilities for articles, and workflows for assigning and moderating updates.

4.1.2.17 Describe any additional features your product has that weren't specifically mentioned above. If there is any additional cost please be sure to describe it here and in the Pricing Form.

4.2 Project Management

Module	Included in Proposal (Y/N)	Individually Licensed (Y/N)	Package Only (Y/N)	Comments (Please list applications that must be bundled with purchase if applicable)
4.2.1 Project Creation and Management				
4.2.2 Collaboration				

4.2.1 Project Creation and Management

4.2.1.1 Describe the process for users to request a project for approval and the approval process within the Solution.

Request:
Approval:

4.2.1.2 Describe the process to create a project within the Solution.

4.2.1.3 Describe the process to create tasks and subtasks within the Solution.

4.2.1.4 Describe how prerequisites and dependencies can be created within the Solution (ie: one task must be completed before the dependent task can be completed).

4.2.1.5 Describe how the Solution supports checking off/completing tasks and subtasks.

4.2.1.6 Describe the capability within the Solution to create notes regarding tasks and/or subtasks.

4.2.1.7 Provide screenshots of the Solution's layout showing a standard task list, including timeline and status.

4.2.1.8 Describe features within the Solution to view the status of a project, including project milestones.

4.2.1.8.1 Describe project status visualization available within the Solution (Ex: bar graphs, charts, etc.).

4.2.1.9 Describe how the Solution tracks expenses, including expenditure amounts and funding sources.

4.2.1.10 Describe how the Solution can track large issues that arise during a project (ex: issues with systems and/or tools that require extensive effort to resolve).

4.2.1.11 Describe how the Solution can house project documentation, such as project charters and change requests.

4.2.1.12 Describe the process to create and use templates for project schedules that can be reused (ex: create a RFP template that can be re-used for future RFPs).

4.2.1.13 Describe the customization of features within the Solution (ie: system administrators turning on and off certain features depending on Member needs).

4.2.2 Collaboration

4.2.2.1 Describe notifications to project team members when a project is created and when tasks are assigned (ie: are emails sent? Are notifications sent within the Solution?).

4.2.2.2 Describe the capabilities within the Solution to tag/mention other users within a task and/or comment.

4.2.2.3 Describe automatic notifications within the Solution that can be set when a task/subtask has been completed.

4.2.2.4 Describe communication features within the Solution (messaging capabilities, etc.).

4.2.2.5 Describe different permissions/visibility available to users based on project and task assignments.

4.2.2.6 Describe reporting functionality available within the Solution, such as how reports are run and what can be tracked through reports (ie: is a project off track, resource management, etc).
How to Run Reports: Report Content:

4.2.2.7 Describe features designed to track work time spent on tasks and projects and calculate associated project costs.

4.2.2.8 Describe any additional features your Solution has that weren't specifically mentioned above. If there is any additional cost please be sure to describe it here and in the Pricing Form.

4.3 Student Safety and Classroom Management

Module	Included in Proposal (Y/N)	Individually Licensed (Y/N)	Package Only (Y/N)	Comments (Please list applications that must be bundled with purchase if applicable)
4.3.1 Classroom Management				
4.3.2 Filtering				
4.3.3 Student Safety				

4.3.1 Classroom Management

**4.3.1.1 Describe how the Solution allows teachers to monitor, restrict, direct, communicate with, and differentiate web activity in real-time for their class of students.

4.3.1.2 Describe how a Teacher can take snapshots of Students' on screen activity, and view Students' past sessions and generate reports.

4.3.1.3 Describe the system's screen mirroring functionality; including pushing content to all devices or sharing content from a remote screen.

4.3.1.4 Describe how class controls may be shared with guest teachers (substitutes or instructional assistants) to leverage the classroom management tools.

4.3.1.5 Describe any differences in features or available tools in the Solution that exist between District-owned/managed devices and Students’ personal devices (i.e., bring-your-own-device programs(BYOD).

4.3.1.6 Describe features to prevent Students from bypassing Teacher controls (blank screen, whitelisted sites, etc.).

4.3.1.7 Describe how Teachers can create, save, and set schedules, policies, and restrictions for individual Students, Classes and/or Groups (eg: table groups within a Class).

4.3.1.8 Please provide the system requirements for the Solution, including any limitations by platform or browser.

4.3.1.9 Describe how a Participant can import and automate the syncing of classes and users in the Solution. **

4.3.1.10 Describe how site administrators, teachers, and parents are associated with Students; and how they are granted permissions to view, manage, and restrict web activity.

4.3.1.11 Please describe any functionality available as part of the core/proposed Solution or as an optional add on/feature that is available for purchase at an additional cost to the Participant. Add all costs to the Optional Costs form in Appendix D.

4.3.1.12 Please also provide a brief description of planned future development that may be beneficial to Participants.

4.3.2 Filtering

4.3.2.1 Describe capabilities of the Solution to allow filter management for blocking/allowing of: URLs, domains and subdomains, images, and/or safe search filtering (Google, Bing, etc.).

4.3.2.2 Describe how the Solution supports differentiated filtering policies (ie: on network v off network, Enterprise asset v personal device, time based policies, in-class/teacher policies).

4.3.2.3 Describe how the filtering capabilities of the Solution categorizes websites and how those categories are leveraged to filter content.

4.3.2.4 Describe how the Solution can support Participants to enforce filters for all Enterprise assets and prevent students from bypassing prescribed filtering (e.g., proxy sites, alternative browsers).

4.3.2.5 Describe a system administrator's reporting capabilities and visibility within the Solution's admin portal (ie: view filtering activities, manage filter settings, etc.).

4.3.2.6 Describe what visibility a Site Administrator has into filtering activities.

4.3.2.7 Describe what visibility and control a parent has into filtering policies and web activity of their student

4.3.2.8 Please describe any functionality available as part of the core/proposed Solution or as an optional add on/feature that is available for purchase at an additional cost to the Participant. Add all costs to the Optional Costs form in Appendix D.

4.3.2.9 Please also provide a brief description of planned future development that may be beneficial to Participants.

4.3.3 Student Safety

**4.3.3.1 Describe the Solution's ability to monitor, detect, and alert the Participant about threats to a student's safety. (ie: self-harm, bullying prevention, threats, etc.).

4.3.3.2 Describe the platforms available to be monitored by the Solution (Google Workspace, Office 365, etc).

4.3.3.3 Describe the process to automate alert notifications, including if they can be programmed to be sent to a hierarchy of specific users and escalated automatically.

4.3.3.4 Describe any automated features for reducing false positives in alerting.

4.3.3.5 Describe the Solution's in-house human monitoring of alerts and hours of availability.

4.3.3.6 Describe the Solution's ability to track network address, geolocation, or other metadata to provide insight into where the activity that triggered the alert may have occurred.

4.3.3.7 Please describe any functionality available as part of the core/proposed Solution or as an optional add on/feature that is available for purchase at an additional cost to the Participant. Add all costs to the Optional Costs form in Appendix D.

4.3.3.8 Please also provide a brief description of planned future development that may be beneficial to Participants.

Part 5 Price

Vendor must complete the Pricing Forms (Appendix D). In Appendix D, Vendor shall detail all costs associated with the proposed Solution, including, but not limited to, the implementation, software licensing and maintenance, training, ongoing support, recommended professional services, taxes and surcharges, and costs of optional services and products. Taxes may be listed as an approximate percentage where appropriate. Costs not identified by Vendor shall be borne by Vendor and will not alter the requirements identified in this solicitation.

	Yes	No	Comments
5.1 Confirm that all costs, including, but not limited to, implementation, software licensing and maintenance, training, ongoing support, recommended professional services, taxes and surcharges, and costs of optional services and products and any other anticipated costs to the Participant have been included on the completed Appendix D: Pricing Form. **			
5.2 Confirm that the Pricing Form includes an itemized schedule of all equipment and software for the proposed Solution and all pricing quoted includes all activities necessary for a complete, turn-key system.**			

5.3 Describe any assumptions made impacting the cost proposal, and any limitations (e.g., professional service hours, number of initial distribution groups) that apply to the listed costs. **

5.4 Provide a narrative explanation of the pricing proposal. Describe in detail any limitations that apply to the proposed pricing (e.g., length of term, service quantities). Note, limitations or terms that are unfavorable may be cause for rejection of the Proposal. **

5.5 Ed Tech JPA reserves the right to award to multiple Vendors a Master Agreement to best meet the needs of its Associate Members. If pricing is contingent upon a specific volume of students or staff or minimum purchase price, explicitly state those conditions. **

5.6 Describe remedies available to Participant if the proposed Solution does not perform as expected. Specifically:

- Software platforms: What refunds or credits would Participant receive if the Solution experiences significant downtime or performance degradation?
- Equipment: What remedies are available if equipment does not perform as expected (including full refunds and/or replacing equipment with different, equivalent products?
- Services: What remedies does Participant have for services that fail to meet the needs of the Participant (e.g., an inexperienced consultant that does not meet Participant expectations)?

5.7 Describe how Vendor addresses disputes related to Solution costs or invoices. Describe how Participate may escalate a concern or invoice dispute.

5.8 Describe how growth and site changes will impact the price.

5.9 Describe how declining enrollment and site changes will impact the price.

5.10 Describe vendor assumptions related to the timing of and terms of payment.

5.10.1 Services (consulting, hosting, project management, implementation/installation): Describe how payment terms are defined relative to the statement of work. For example, confirm whether an initial, up-front payment is required before work begins (e.g., 10% of the total project costs) or whether all costs will be invoiced on a time and materials basis after work has been completed. Confirm whether payments are tied to specific time intervals (annual, monthly), milestones (completion of development phase), or actual service hours (number of consultant hours used during past 30 days).

5.10.2 Software: Confirm when annual licensing and support costs begin (e.g., at project initiation or only after the Solution is "live" and in productive use).

5.10.3 Equipment: Confirm when invoices are sent and payment expected for invoices (e.g., net 30 days from invoice date, where invoices are generated after delivery of equipment). Describe the process to

extend the invoice deadline if needed (e.g., Participant is unable to verify equipment is working/acceptable due to partial deliveries/missing components).

5.11 Please describe if any implementation/training costs apply for Members who are continuing use of the same Solution (Ex: Member A previously used the Solution using a RFP they issued as a procurement vehicle. Their agreement expires and they purchase the Solution for a new term using the Ed Tech JPA agreements resulting from this RFP, but desire to use their previous instance for the same Solution).

Part 6 Exceptions

Describe any exceptions to the RFP content, general expectations, specific requirements, and/or the Ed Tech JPA's standard Master Agreement and Purchase Agreement. For each exception, propose acceptable alternative language and/or provide rationale to support the exception. Proposed exceptions must be addressed by Vendor and agreed upon by Ed Tech JPA during contract negotiations to be effective. Ed Tech JPA may elect not to award and/or to revoke award based on requested exceptions that cannot be agreed upon.

*** End of Proposal Form ***