MARICOPA COUNTY COMMUNITY COLLEGE DISTRICT

REQUEST FOR PROPOSAL #3466-6

Employee Wellness Platform

Proposal Due Date

September 16, 2020 (local time)

MARICOPA COUNTY COMMUNITY COLLEGE DISTRICT

RFP # 3466-6

Employee Wellness Platform

SCHEDULE OF EVENTS

ACTIVITY	DATE
Release RFP	August 17, 2020
Questions Due	August 27, 2020
Proposals Due	September 16, 2020
Proposed Contract Award	October 2020

Table of Contents

MARICOPA COMMUNITY COLLEGES

ACKNOWLEDGMENT OF RECEIPT
RFP # 3466-6
Employee Wellness Platform

Please provide the requested information below as acknowledgment that you have received our Request for Proposal noted above. To ensure receipt of any future addenda and to remain in our vendor database it is strongly recommended that interested Bidders complete this acknowledgment and return via email to larry.woo@domail.maricopa.edu even if you do not intend to submit a proposal.

All addenda/amendments will continue to be posted on our website at: https://procurement.maricopa.edu/

Failure to sign and return the "Acknowledge of Receipt" will result in your company not being sent any addenda to this RFP. Addenda may significantly alter the specifications of this RFP which could result in your proposal being deemed unresponsive if this form is not returned.

Name of Firm: _____

Address: _____

_____

_____

Tel #: _____ Fax #: _____

E-Mail: _____

Name: (Print) _____ Title: _____

Signature: _____ Date: _____

PLEASE NOTE: Failure to respond to this acknowledgement **may** result in your company's removal from our vendor database for this commodity.

( ) We will not be responding to this solicitation please retain us on the Proposing Firm's mailing list.

GENERAL

1.1 INTRODUCTION

Maricopa County Community College District (MCCCD) is seeking proposals from qualified firms for an Employee Wellness Platform that can help enhance the overall health and wellness of its employees and is customizable to MCCCD's needs. The platform should engage and motivate employees on topics such as Nutrition, Fitness and Mental Health through various challenges and/or campaigns.

1.2 MCCCD DISTRICT MAKE-UP

MCCCD comprised of ten colleges, and numerous education centers dedicated to educational excellence by meeting the needs of the businesses and the citizens of Maricopa County. Each college is individually accredited, yet part of a larger system, the Maricopa County Community College District (MCCCD or District). The MCCCD is one of the largest higher education systems in the nation. As the largest provider of health care workers and job training in Arizona, it is a major resource for business and industry and for individuals seeking education and job training. More than 200,000 students attend the Maricopa Community Colleges each year taking credit and non-credit courses. MCCCD employs nearly 4,500 full-time faculty and staff and more than 9,000 part-time faculty and staff.

1.3 HISTORY

MCCCD ranks as one of the nation's largest systems of its kind and is the largest single provider of higher education in Arizona. MCCCD educates and trains thousands of students year-round. What's more, thousands of employees from both local and relocating businesses and industries are enrolled in customized workforce training programs with the MCCCD system. MCCCD's administration, faculty and staff are committed to working collectively and responsibly to meet the life-long learning needs of our diverse students and communities.

A seven member governing board governs MCCCD. Five members are elected from geographical districts within Maricopa County, while two are elected on a countywide basis. The chief executive officer of MCCCD is the Chancellor; and a president heads each of the colleges. MCCCD is a political subdivision of the State, and the elected governing board has the power to levy taxes. Funding comes from property taxes, student tuition, and federal, state and private grants.

1.4 CURRENT ENVIRONMENT

The Maricopa County Community College District, along with most educational entities in the State of Arizona, has been dealing with decreased funding support from the State for many years. In 2015, the State of Arizona eliminated all of the funding it was providing to help support MCCCD's operations. In addition to the loss of all funding from the State, MCCCD has experienced a decrease in student enrollment, which is a typical trend for all community colleges during strong economic times.

It is the philosophy of MCCCD that this loss of funding and decreased enrollment should not be bridged by raising student tuitions or by burdening the public with increases in their taxes. The result of these funding reductions has created a need to rethink the traditional model of customer and vendor so that MCCCD can continue to provide the best learning environment for our student population as well as practice good stewardship of the public support we receive.

It is the District's desire to move towards a model that is being utilized by many other higher learning institutions throughout the country which is to evolve the previous customer/supplier relationships associated with our contractors to that of becoming our Strategic Partners. By cultivating strategic partnerships it will enable MCCCD and the awarded contractor to help identify potential cost reductions, maximize efficiencies, and tap unexplored value-added opportunities to maximize resources and support to the benefit of both parties. Any potential strategic initiatives can be established during negotiations.

1.5 STRATEGIC PARTNERSHIPS

In addition to providing the services listed in this Request for Proposal, MCCCD is continually seeking to expand its relationships with contractors who can evolve into a strategic partner. We are seeking companies that can help expand the boundaries of what has been thought of as traditional staffing contracts by infusing the program with new concepts, out-of-the box thinking, and value-added offerings that may not have existed before.

It is recommend that you review our 2017 – 2020 Strategic Commitments and detail in your proposal how leveraging a strategic partnership with your company can assist MCCCD in achieving our goals. A copy of these commitments can be found using the link below:

https://procurement.maricopa.edu/sites/procurement/files/purchasing/forms/MCCCD%20Strategic%20Commitments%202017-2020%20-%20Nov%2015%2C%202016.pdf

1.6 VALUE ADDED OFFERINGS:

MCCCD would be interested in receiving any suggestions that would bring added value to this contract. As stated in section 1.4, the previous sources of State revenue support have been cut and in order to continue to provide the quality of education our students deserve MCCCD is open to considering new resources and ideas to help alleviate these short-falls. These proposals may be a one-time occurrence or recurring in nature, revenue producing (such as incentives or rebates) or other offerings that would bring added value to our organization. Provide details how leveraging a strategic partnership with your company can assist MCCCD in achieving our goals. Creative solutions are encouraged and should be clearly labeled in the proposal as an attachment.

Potential value added offerings may be proposed in general in the attachment but will not be reviewed and considered until after the competitive evaluation process has been completed. Once a susceptibility of award is determined by the evaluation team further negotiations regarding these added value offerings may occur and must be completed prior to a final contract award.

The negotiation of any of these offerings is separate from the evaluation process. Changes / additions to these offerings may be made if agreed upon in writing by both parties and included as a signed contract amendment.

MCCCD reserves the right to exclude items offered under this section from co-operative use unless also agreed upon by the awardee.

PROPOSAL INSTRUCTIONS

2.1 PURPOSE OF RFP

Maricopa County Community College District is seeking proposals from qualified firms for an Employee Wellness Platform to be used by MCCCD employees in accordance with the Scope of Work specified in this RFP.

2.2 PROPOSAL QUESTIONS

All questions regarding this Request for Proposal should be directed to:

Larry Woo
(480) 731-8521
E-Mail: larry.woo@domail.maricopa.edu

Questions must be sent by e-mail. Questions will only be accepted until 3:00 p.m. (local time), August 27, 2020. We will not respond directly to the company asking the question. All questions received within the question period will be acknowledged even if an answer cannot be provided. Responses to the questions received by the deadline will be answered in the form of an addendum and sent to all known potential respondents, based on returned Acknowledgement of Receipt forms, on/about September 2, 2020.

2.3 PROPOSAL SUBMISSION

It shall be the responsibility of the Proposer to assure that Proposals are received as follows:

Due to the ongoing COVID-19 health situation all proposals must be submitted electronically via email. Proposals must be combined into a single, complete PDF document with all tabs, attachments, etc. in the order listed in Section 4.5. Do not submit a proposal with the required sections/tabs separated into individual PDF documents. All required items of the proposal should be submitted on a single PDF file with the exception of a HECVAT Lite submission which may be in a separate Excel file.

The Proposals must be emailed to: larry.woo@domail.maricopa.edu. The official submittal time of record will be the time stamp from the MCCCD email server. The email time stamp must read no later than 3:00 p.m., Wednesday, September 16, 2020. Proposals received after this time and date shall not be considered and will be returned unread. **When submitting your proposal please allow enough time in case of internet outages or other technological issues that may cause an issue in its delivery. It is your responsibility to submit your proposal with enough lead-time to account for any delay.** An email will be sent acknowledging receipt of your submission as soon as possible.

The subject line of your email should include the first line of the information below:

Request for Proposal # 3466-6, Employee Wellness Platform

Proposal Closing Date: September 16, 2020 Time: 3:00 p.m. (Local Time)

NOTE: MCCCD email restricts attachments over 25MB. If your proposal's PDF file is larger than 25MB you will need to compress it or use a zip file program to reduce it down to an acceptable size. The only exception to the one PDF file would be if you must divide the proposal into smaller file sizes and send it in multiple emails due to being unable to compress your file size to under a 25MB attachment. In either case, you are responsible to submit your proposal in its entirety by the deadline time and date listed.

Before submitting your proposal make sure you have read, understand, and comply with Part IV – Proposal Requirements, Paragraph 4.2 – Deviations from RFP.

2.4 AWARD DETERMINATION

This Request for Proposal does not constitute a commitment by the District to award a contract. The District reserves the right to waive any informalities and to reject any or all proposals and/or to cancel the Request For Proposal. The award shall be made on the proposal(s) that serves the best interest of the District and will not be evaluated solely on a monetary basis. The District reserves the right to negotiate a contract with the selected awardee. Even after the execution of a contract document or Notice of Award, the selected vendor may not initiate contract performance or incur any contract costs until it receives a District-issued purchase order or Procurement card.

2.5 PROPRIETARY INFORMATION

In the event any Proposer shall include in the Proposal any information deemed "proprietary" or "protected", such information shall be separately packaged from the balance of the proposal and clearly marked as to any proprietary claim. Unless it is critical for the evaluation of a proposal, the District discourages the submission of proprietary information and undertakes to provide no more than reasonable efforts to protect the proprietary nature of such information. The District's Purchasing Manager will review all proprietary information after the proposals are opened and, in conjunction with District General Counsel, make a determination if the information provided meets the classification as proprietary. If the information cannot be classified as proprietary by the District, the Proposer shall be notified and provided to the opportunity to redact that information from their proposal. Any redacted information will not be considered when evaluating the proposal. The District shall have the right to use any or all information included in the proposals submitted unless the information is expressly restricted by the Proposer.

2.6 PROPOSAL FORM

All proposals must be submitted in writing. Oral, telephone, facsimile (fax machine) or computer data transfer proposals will not be accepted. Each proposal shall be prepared simply, providing the

straightforward, concise description of the proposer's ability to meet the requirements of the RFP. Emphasis should be on completeness and clarity of contents and should try to limit the proposal to fifty (50) typewritten pages in length plus any pricing schedule(s), exhibits, resumes, proposed draft revenue sharing agreement, or attachments.

2.7 PROPOSER MODIFICATIONS TO PROPOSALS

No modifications to proposals are permitted by the proposer after the published RFP opening date and time. Proposals may be modified after delivery, but before opening, by requesting that they be returned. Modifications must be made and the response returned by the published date and time.

2.8 WITHDRAWAL OF PROPOSAL

Any Proposer may withdraw their proposal by written request at any time prior to the deadline set for receipt of proposals. No proposal may be withdrawn or modified after that deadline and shall be binding upon Proposer for a period of ninety (90) days after due date. Withdrawn Proposals may be resubmitted up to the time designated for the receipt of Proposals provided that they are then fully in conformance with the general terms and conditions of the RFP.

2.9 PROPOSAL COSTS

Any and all costs associated with the preparation of responses to this Request for Proposal, including site visits, oral presentations and any other costs shall be entirely the responsibility of the Proposer and shall not be reimbursable in any manner.

2.10 ORAL PRESENTATIONS

Proposers may, after opening and prior to award, be required to make oral and visual presentations at the request of the MCCCD. The MCCCD will schedule the time and location for any presentations as requested. Oral presentations will be evaluated.

2.11 AWARD WITHOUT DISCUSSION

The MCCCD reserves the right to make an award(s) without further discussion of the proposals received. It is therefore critical that all proposals be submitted initially in the most favorable terms possible, both economically and technically.

2.12 CONTRACT COMMENCEMENT/TERM

It is the intent of the District to issue a 5-year contract with an anticipated commencement date of January 1, 2021. A written Notice of Award with a specific contract start date will be made prior to commencement of performance. MCCCD may, at its discretion and with the concurrence of the

successful proposer, extend the contract if a mutually advantageous strategic agreement can be reached that would benefit from a longer term.

2.13 MCCCD MODIFICATIONS TO PROPOSALS

Any interpretation, correction, or change of this RFP will be made by written Addendum. Interpretations, corrections, or changes of this RFP made in any other manner will not be binding, and Proposers shall not rely upon such interpretations, corrections, and changes. Any changes or corrections will be issued by MCCCD Purchasing. Addenda will be mailed or faxed to all that are known to have received a copy of the RFP. Addenda will also be posted to the proposal documents on the Purchasing website located at www.maricopa.edu/purchasing.

2.14 NON-COLLUSION

The MCCCD encourages free and open competition. Whenever possible, specifications, proposal invitations and conditions are designed to accomplish this objective, consistent with the necessity to satisfy the MCCCD's needs and the accomplishment of a sound economical operation. The Proposer's signature on its proposal guarantees that any prices offered have been established without collusion with other eligible Proposers and without effort to preclude the MCCCD from obtaining the most advantageous proposal.

SCOPE OF WORK/SPECIFICATIONS

The following Scope of Work outlines the expected areas of service and interaction requested by MCCCD of an Employee Wellness Platform provider.

Employee Engagement

Provide a wellness platform that can enhance MCCCD's Wellness Culture by engaging and motivating employees.

Provide a wellness platform that includes behavior change campaigns and/or challenges.

Provide a wellness platform that is customizable for our participants.

Wellness Program Administration

The wellness platform is easy to administer and has an easy to use interface for tracking employee engagement.

The wellness platform allows new hires to be enrolled with a data file upload in common data formats.

The wellness platform allows employee data to be changed through a data file upload in common data formats.

The wellness platform shows employee engagement by college and by the district as a whole.

Health/Wellness Content Selection and Communication

The wellness platform includes content experts delivering tools and resources on the following topics: Nutrition, Fitness and Mental Health.

The wellness platform allows MCCCD to determine what content is available to employees.

Email communications to employees from the wellness platform is controlled by MCCCD.

PROPOSAL REQUIREMENTS

Paragraphs 4.1 & 4.2 below require specific, written responses or confirmations. To be considered for selection, respondents shall meet/provide the following requirements:

4.1 MINIMUM REQUIREMENTS

- 4.1.1 Must be licensed by the State the business is in, if services requested require such licensure.
- 4.1.2 Must provide a completed Pricing Schedule (Section 7) signed by an authorized company signatory.
- 4.1.3 Must have carefully read and understand all parts of the RFP and certified that the Proposal is made in accordance therewith.
- 4.1.4 Must submit written answers to the Respondent Questionnaire (Section 5). All answers must be in the order in which the questions were asked.
- 4.1.5 If the Proposer will be hosting MCCCD confidential information, the Proposer must provide one of the accepted privacy/security audits as part of Attachment B; or complete and provide the Higher Education Cloud Vendor Assessment Tool (HECVAT) found at https://library.educause.edu/resources/2020/4/higher-education-community-vendor-assessment-toolkit. Blanks or simple "no's" or "yes's" are not acceptable. Some explanation is required. You may submit the "Lite" version of this tool (see Attachment C)

4.2 DEVIATIONS FROM RFP

Proposers must specifically provide a separate listing under Tab 8 of your proposal for each circumstance in which their proposal differs from any terms or conditions of this Request for Proposal. Failure to list such a deviation will result in the terms of the proposal being disregarded in favor of the corresponding term(s) of the RFP. Material deviations from the requirements of this RFP shall result in rejection of the proposal.

The term "material deviations" includes both deviations from the MCCCD contract terms set forth in this RFP **and** additional contract terms that the Proposer requests the MCCCD to consider. Be aware that the absence of a term on a subject in the RFP, particularly a general contract term and condition, does not mean that the Proposer should feel free to offer one. The MCCCD considers the General Terms and Conditions of this RFP to be a fair allocation of risk between a contractor and the MCCCD. It will not accept terms – revised or additional ones - that shift those risks or provide the Proposer with additional discretion. The Proposer in choosing the respond to this RFP, must demonstrate in its Proposal that it accepts the terms upon which the MCCCD is conducting the competition.

The Proposer must list in the separate listing specified above all deviations, including any additional terms, in its Proposal so that MCCCD may consider them in determining the most advantageous offer. Deviations that a winning Proposer submits after it has been selected for award, such as through a vendor standard template contract, will not be considered.

4.3 SIGNATURE

The Contractor shall furnish and include all requested information with their proposal. Statements are required to be complete and accurate, and the proposal shall be signed by an authorized signatory of the company (sworn to and notarized, if requested). A proposal submitted by an agent will have a current Power of Attorney attached certifying the agent's authority to bind the Proposer. Omission, inaccuracy, or misstatement may be sufficient cause for rejection of the proposal.

4.4 AWARD CONSIDERATION

From the total information requested, determination shall be made of the Proposer's ability to serve the MCCCD. Only proposals from responsible organizations or individuals, as determined by the MCCCD, which have the capability of providing the required services under this RFP, shall be considered. Representatives from the MCCCD reserve the right to conduct interviews with the individual proposers for clarification of the proposals presented. The MCCCD reserves the right to negotiate any and all provisions presented in the proposals.

4.5 FORMAT & SUBMITTAL REQUIREMENTS BOUND AND TABBED AS FOLLOWS

Tab 1: Price Totals Sheet / Itemized Price List
Tab 2: Signature Page
Tab 3: Scope of Work
Tab 4: Respondent Questionnaire
Tab 5: Attachment A & B (including privacy/security audit report)
Tab 6: Warranty (if required)
Tab 7: Signed Addenda (i.e.-addenda acknowledgments if any)
Tab 8: Deviation to Terms and Conditions (if any)
Tab 9: HECVAT Lite-Higher Education Community Vendor Assessment Tool (if needed)

RESPONDENT QUESTIONNAIRE

Provide information to all sections below. Failure to provide required information may cause the proposal to be deemed non-responsive.

General Information

5.1. Provide a brief history of your company and the services it provides, specifically as it relates to managing a wellness platform.
5.2. Why should MCCCD choose your platform and your company? Provide a concise narrative as to why your product and your company are best able to serve MCCCD. Include any key items about your company and unique features of your product that distinguishes it above others.
5.3. Has this platform been used at similar size organizations? Has it been used at similarly structured institutions of higher education?

Wellness Philosophy

5.4. Provide a detailed description of your wellness platform.
    a. Explain how your platform supports the individual employee in each of the eight dimensions of wellness: social, spiritual, financial, occupational, emotional, social, environmental and physical.
    b. Explain how your program supports MCCCD to create, support and sustain a well-organization.
5.5. Describe how your company differentiates itself and its platform within the marketplace.
5.6. How is lifestyle/behavior change embedded into your product offering?
5.7. Does your program allow for family members and friends to participate in programs at no charge?

Personalization and Integration

5.8. Describe how your platform works to promote engagement to employees based on their individual goals, interests and health profiles.
5.9. Describe how programs are promoted to specific employees, based on their goals, interests or health concerns.
5.10. Describe your platform's ability to export participant biometric completion into our Human Capital Management (HCM) program.
5.11. Outline your platform's ability and any constraints, to integrating existing data from our third-party systems and vendors with your platform.
5.12. Describe how your platform interfaces with external health and wellness vendors?
5.13. Describe how your platform integrates with other online and mobile app health/activity trackers?

5.14. Describe what programs you have directly integrated into your platform?

5.15. Describe your platform's use of templates and style sheets and provide screenshots. Describe how MCCCD can theme the system, and the extent to which users may customize or be prevented from customizing the interface.

5.16. Describe the process to accept eligibility feeds from our organization to use in verifying participant eligibility when registering for a screening?

5.17. Describe any interaction or interface with external sources including social networking tools, apps, and interactive devices/smartwatches (i.e., Fitbit, Apple Watch, etc.).

Challenges and Competitions

5.18. Are your challenges team-based or individual-based?
   a. Describe the process for our Wellness Coordinators to set up a team or business – unit to business – unit challenge.
   b. Describe the process for an individual to set up a challenge and invite others.

5.19. Can participants interact with challenges through the online platform and through a mobile app?

5.20. Describe the platform's ability to engage, motivate and communicate with participants during a challenge?
   a. Describe the role of our Wellness Coordinators in this process.

5.21. List challenges your platform offers aside from physical activity challenges?

5.22. Does our organization have the ability to create and implement custom challenges?

Incentive Management

5.23. Does your platform provide incentive administration and fulfillment capabilities?
   a. Describe the various types of incentives available to participants and all methods of member redemption and administration for our organization
   b. Describe incentive fulfillment options (cash, gift card, plan design features such as deductible waiver or insurance premium reduction). Are incentives customizable to our organization?

5.24. Does your platform track incentives in dollars or points?

Customer Service

5.25. Do you have an in-house customer service center to support our participants? What city/state are they located in?
   a. Describe the customer service support provided before, during, and after a participant is enrolled.

5.26. How do you handle customer service staffing during initial enrollment, annual/open enrollment or other peak times?

5.27. Describe the training provided to your customer service representatives.
5.28. Is your customer service available via chat?
5.29. What hours is your customer service available?

Account Management

5.30. Will an account manager who has day-to-day account responsibilities be assigned to our account? If so, what city and state will they be located in?
5.31. Will the same account manager assigned during implementation be the one handling future day to-day administration?
5.32. What changes in the account management structure or personnel occur as we move from program implementation to ongoing support?

Implementation

5.33. Describe the in-house team that manages implementation. Is your platform development team completely in-house? What city and state are they located in?
5.34. Will you assign a designated implementation manager to manage our implementation? If so, what city/state will they be located in?
5.35. Describe in detail the timeline from initial creation to deployment (keeping in mind the January 1, 2021 go live date).
5.36. Identify any recommended MCCCD resources (i.e.-personnel or technology needs) needed for implementation.
5.37. Do you require a standard eligibility file or can you accept data in any format? If a standard file is required, provide a copy of the file layout and requirements.
5.38. How often can you update eligibility?

Marketing

5.39. Describe your communication strategy to notify and engage eligible members about our wellness platform.
    a. Prior to implementation
    b. During implementation
    c. Periodic
    d. Annual
5.40. Describe the in-house team that manages communications and how they will work with our organization.

Analytics and Reporting

5.41. Describe in detail standard management outcome reports for both the organization and the employee/participant. Include samples.

5.42. Describe your platform's ability to export aggregate information to our organization.
5.43. Do you provide quarterly, semi-annual, or annual reports that identify, among other things, utilization trends and/or benchmarks?
5.44. Describe your platform's ability to provide aggregate reports to our organization illustrating the positive health impacts of the program.
5.45. Does your platform have the ability to report on engagement in a defined segment within our organization such as individual Colleges?
    a. Do we have the ability to run our own reports with a Dashboard?
    b. Are reports available on demand?
5.46. Which data points can be identified and reviewed?
5.47. Describe your analytics capabilities, including the level of custom ROI/VOI analysis you provide.

Technology

5.48. Do you offer a mobile app for employees? If so, does your mobile app provide the same depth and breadth of functionality as your web app?
5.49. What tools do you offer for participants to take verified biometric readings?
5.50. Describe your platform's ability to upload biometric results from a third-party vendor?
5.51. Describe how the proposed system will provide a high-availability service. Is the system scalable and/or able to add additional processing power on-demand? How do you manage a high-demand spike?
5.52. Briefly describe your internal backup and disaster recovery procedures, provide a sample disaster recovery plan.
5.53. How many different authentication methods can be used on the same system and what methods of authentication can be used?
5.54. When there is a security issue or immediate fix needed, what is the average turnaround time for a patch / hotfix to be released?
5.55. If cloud-based, how does the cloud-based system provide for high performance regardless of use?
5.56. What are the alerts or warnings you provide to your customers when issues arise?
5.57. Describe how your product supports large data volumes including large database/application server messaging and high arrival rates (include limitations).
5.58. Describe your company's standard service level agreement for system uptime, problem resolution, etc. Please include time to resolve and also include your responsibilities and MCCCD responsibilities for problem resolution.
5.59. Describe the data center that would house MCCCD's environment. Include information on security, network infrastructure, servers, etc.
5.60. For the purposes of calculating the uptime guaranteed in the SLA, what is your definition of when a system is "down" or not available?
5.61. Describe possible methods for how MCCCD would be compensated for any failure to meet the SLA requirements?
5.62. When system performance is poor what tools does your team use to monitor the system and be alerted to the performance problem?

Privacy

5.63. Explain how your platform is secure and HIPAA compliant. Describe in detail your system security capabilities including compliance with State and Federal regulations.

NOTE: When responding to this section, clearly identify in your proposal response each paragraph number shown above and your response to that paragraph.

EVALUATION CRITERIA

The following is a listing of general and specific criteria used for the evaluation of this RFP. The areas include, but are not limited to:

6.1 General quality of responsiveness of proposer:

- A. Ability to meet all terms and conditions
- B. Completeness and thoroughness of proposal
- C. Grasp of scope of work to be performed
- D. Description of approach to be taken
- E. Evidence of effective organizational and management practices
- F. Qualifications of personnel
- G. Experience and past performance

6.2 Specific areas that will be evaluated and scored except as described in STEP THREE below:

- A. Past experience in providing comparable services to other clients.
- B. Responses to Minimum and Specific Requirements.
- C. Respondent Questionnaire responses.
- D. Pricing.
- E. Sustainability (if applicable)

Proposals will be evaluated in accordance with the following three-step process:

STEP ONE - Verification of each proposer's compliance with the RFP general terms and conditions as listed in Section 1, 2 and 3 of this RFP.

STEP TWO - Verification of each proposer's compliance that all required written responses/confirmations are thoroughly submitted.

STEP THREE – All proposals meeting the criteria as presented in Steps One and Two will be evaluated with a "points-earned compliance matrix". An evaluation committee will evaluate and score the proposals. The proposals will be ranked on a "points-earned" technical, service and financial compliance matrix. The evaluation committee may continue to evaluate proposals after the initial scoring of them by any means that it deems reasonable. If the evaluation committee schedules oral presentations, the presentations may or may not be scored and that scoring may, but is not required to be added to the previous scoring of the proposals. The evaluation committee reserves the right to use additional advisory committees or subject matter experts at any time during this RFP to assist with the evaluation.

PRICING SCHEDULE

The undersigned has read and understands all conditions and terms of RFP 3466-6, is authorized to submit this proposal on behalf of the company, and hereby offers to perform the services for the pricing indicated below:

7.1 Products/Services as requested in this RFP:

Pricing for Wellness Platform	**Proposed Pricing**
Annual Hosting and Maintenance	
Administration Fee (PEPM)	
Challenges	
Special Projects	
Other:	
Additional/Optional Services (if any):	**Proposed Pricing**

7.2 Prompt Payment Discount (if offered): _____

Costs/Fees listed above shall include all overhead and profit. No billing will be accepted that shows any other costs than those listed above. This includes, but is not limited to, travel, any out-of-pocket costs, meetings, secretarial, printing, delivery, rent, phone calls, postage, overnight mail service, accounting, fuel charges, office supplies, etc.

You may submit a more detailed pricing schedule in lieu of the above as an attachment to this page, but the signature page (Section 10) must be completed, signed and included with your proposal.

SPECIAL TERMS AND CONDITIONS

Any deviations to the Special Terms and Conditions **MAY be considered in this proposal**

These General Terms and Conditions, the other provisions of the RFP and amendments to it, the Proposer proposal, and MCCCD's purchase order terms ("Contract Documents") along with any engagement letter will constitute the provisions of the contract between MCCCD and successful Proposer ("Contract"). MCCCD reserves the right to negotiate with the successful Proposer and modify any of the provisions of the Contract upon mutual written agreement of the parties. The RFP, amendments to it, and MCCCD's purchase order terms will take precedence over any inconsistent terms in a proposal or other documents. The term "days" as used in this Contract means business days, unless otherwise specified.

8.1 INSURANCE REQUIREMENTS

Contractor shall maintain during the term of this Agreement insurance policies described below issued by companies licensed in the State of Arizona or hold approved non-admitted status on the Arizona Department of Insurance List of Qualified Unauthorized Insurers. Insurers shall have an A.M. Best rating of A - VII or better. At the signing of this Agreement, Contractor shall furnish the MCCCD with certificates of insurance evidencing the required coverages, conditions, and limits required by this Agreement. Certificate of Insurance shall be sent to:

Representative's Name (person who is collecting the certificate)

College or District Office and address

Phone number and email address

The insurance policies, except Worker's Compensation, must be endorsed as require by this written agreement to name MCCCD and its agents, officers, officials, employees, and volunteers as additional insureds or its equivalent:

The Maricopa County Community College District and its agents, officers, officials, employees, and volunteers are hereby named as additional insureds as their interest may appear.

The insurance policies shall contain a waiver of subrogation endorsement in favor of Maricopa County Community College District, its agents, officers, officials, employees, and volunteers for losses arising from work performed by or on behalf of the contractor.

Contractor and, if applicable, any subcontractors will notify the MCCCD Risk Manager by certified mail promptly if it receives notice or the expiration, cancellation, suspension, or material change in its insurance coverage, but in no case fewer than 30 days before the action specified in the notice. The

Contractors insurance must be primary, and any insurance or self-insurance maintained by MCCCD will not contribute to it. If any part of the Agreement is subcontracted, these insurance requirements also apply to all subcontractors.
The contracting College or District Office, in consultation with MCCCD Risk Management, reserves the right to review or make modifications to the insurance limits, required coverages, or endorsements throughout the life of this contract, as deemed necessary. Such action between the College or District Office and MCCCD Risk Management will not require a formal Contract amendment but may be made by administrative action.

In the event any professional liability insurance required by this Contract is written on a "claims made" basis, Contractor warrants that any retroactive date under the policy shall precede the effective date of this Contract; and that either continuous coverage will be maintained or an extended discovery period will be exercised for a period of three (3) years beginning at the time work under this Contract is completed. Contractor's work or services and must be evidenced by annual certificates of insurance. Contractor shall notify the MCCCD Risk Manager by certified mail promptly if it receives notice or the expiration, cancellation, suspension, or material change in its insurance coverage, but in no case fewer than 30 days before the action specified in the notice. The Contractor's insurance must be primary, and any insurance or self-insurance maintained by MCCCD shall not contribute to it. If any part of the Contract is subcontracted, these insurance requirements also apply to all subcontractors.

Commercial General Liability (CGL) – Occurrence Form
Policy shall include bodily injury, property damage, and broad form contractual liability coverage, including but not limited to, the liability assumed under the indemnification provisions of this Contract.

- General Aggregate $2,000,000
- Products – Completed Operations Aggregate $1,000,000
- Personal and Advertising Injury $1,000,000
- Damage to Rented Property $50,000
- Each Occurrence $1,000,000

If applicable, **Commercial Automobile Liability** insurance with a combined single limit for bodily injury and property damage of not less than $1,000,000.00 each occurrence with respect to the Contractor's and, if applicable, the sub-contractor's owned, hired, and non-owned vehicles.

Worker's Compensation insurance with limits statutorily required by any Federal or State law and Employer's Liability insurance of not less than $1,000,000 for each accident, $1,000,000 disease for each employee, and $1,000,000 disease policy limit.

If applicable, **Professional Liability** insurance covering acts, errors, mistakes, omissions rising out of the work or services performed by the Contractor, or any person employed by the Contractor, with a limit of not less than:

- Each Claim $2,000,000
- Annual Aggregate $2,000,000

Network Security and Privacy Liability coverage in an amount not less than $2,000,000 per claim and annual aggregate, covering all acts, errors, omissions, negligence, infringement of intellectual property (except patent and trade secret); network security and privacy risks, including but not limited to unauthorized access, failure of security, breach of privacy perils, wrongful disclosure, collection, or other negligence in the handling of confidential information, privacy perils, and including coverage for related regulatory defense and penalties; data breach expenses, in an amount not less than $2,000,000 and payable whether incurred by MCCCD or Contractor including but not limited to consumer notification, whether or not required by law, computer forensic investigations, public relations and crisis management firm fees, credit file or identity monitoring or remediation services in the performance of services for MCCCD or on behalf of MCCCD hereunder. The policy shall include coverage for third party claims. The policy shall contain an affirmative coverage grant for contingent bodily injury and property damage emanating from the failure of the technology services or an error or omission in the content/information provided. Such insurance shall be maintained in force at all times during the term of the agreement and for a period of three years thereafter for services completed during the term of the agreement. MCCCD shall be given at least 30 days' notice of the cancellation or expiration of the aforementioned insurance for any reason.

8.2 OBLIGATIONS TO PROTECT CONFIDENTIAL INFORMATION

MCCCD information that is required to be kept confidential will be kept so in perpetuity.

For purposes of this Contract, Confidential Information is defined as any and all MCCCD information and data whose collection, sharing, dissemination, use, preservation, disclosure, protection, storage, destruction and/or disposition is governed by federal, state, local and/or international law or regulation, or by contract. Confidential Information includes, but is not limited to, Social Security Numbers, student records, student financial records regarding students (or their parents or sponsors), financial and personal information regarding MCCCD employees and students, protected health information (as defined by the Health Insurance Portability and Accountability Act of 1996 and its regulations), and other personal information relating to an identified or identifiable natural person. In addition, Confidential Information includes business and marketing plans, strategies, data, technology and technical information, access credentials, system information, institutional financial and performance records and other information that is proprietary to or developed by MCCCD.

8.2.1 Confidential Information does not include (i) information the receiving party already knows, (ii) information that becomes generally available to the public except as a result of disclosure by the receiving party in violation of this Contract, and (iii) information that becomes known to the receiving party from a source other than the disclosing party on a non-confidential basis. . If Contractor is required by law to transfer, disclose or permit access to or use of Confidential Information by a third party, Contractor will promptly notify MCCCD in advance of such action and cooperate with MCCCD to limit the extent and scope of such transfer or disclosure.

8.2.2 If the Contractor potentially has access to MCCCD Confidential Information under this Contract, Contractor agrees that Confidential Information provided to it, or to which it may

have access, during the provision of service, will be used only and exclusively to support the service and service execution and not for any other purpose. Contractor agrees that Confidential Information will not be further disclosed to any third-party without the express written consent of MCCCD. Such use will not include examining data for targeted marketing either within the confines of the service or external to the service (e.g., keyword indexing). Contractor may use aggregate statistics on service usage solely for internal business purposes to enhance or optimize the functionality of the service provided under the Agreement provided that such data cannot be attributed to any individual following anonymization and aggregation and no MCCCD Confidential Information is retained by Contractor.

8.2.3 Contractor will limit access to Confidential Information to its employees with a need to know the Confidential Information to carry out the activities under this Contract and will instruct those employees to keep the information confidential. It is understood, however, that Contractor may disclose the MCCCD Confidential Information on a need-to-know basis to its contractors, subcontractors, and vendors who are performing services, provided those contractors, subcontractors, and vendors have executed confidentiality agreements and have agreed to materially the same or greater security obligations as Contractor provides with respect to MCCCD Confidential Information hereunder, and further provided that Contractor shall remain legally and financially liable for any unauthorized disclosure of the MCCCD Confidential Information by those contractors, subcontractors, and vendors. The access rights of any employees, contractors, and subcontractors will be removed immediately by Contractor upon termination or adjusted upon change in job function when such access is no longer necessary. Contractor will closely monitor physical and logical access to Confidential Information, including areas where it stores Confidential Information. Without limiting the foregoing, Contractor shall maintain and only allow access to Confidential Information in the United States. Contractor shall obtain MCCCD's written consent prior to allowing access to Confidential Information from outside the United States, or transferring systems containing Confidential Information outside the United States.

If a Contractor staff person or Contractor subcontractor potentially will have access to MCCCD's network, facilities, data, Confidential Information, and/or Sensitive Information,[1] they may not perform any work involving such access until they have received MCCCD's privacy and security training, and/or accepted and agreed to adhere to MCCCD's privacy and security policies and procedures and have

[1] Sensitive Information is information that is so deemed under applicable law. Personally identifiable information, personally identifiable education records, individually identifiable health information, personally identifiable financial information and payment card information are examples of Sensitive Information covered under the Arizona Revised Statutes (ARS), Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act of 1996 (HIPAA), Gramm–Leach–Bliley Act (GLBA aka Financial Services Modernization Act of 1999) and Payment Card Industry Data Security Standard (PCI DSS), respectively.

entered into a non-disclosure agreement with MCCCD. [2] If exigent circumstances are presented, all or part of this requirement may be waived in writing by MCCCD's Chief Privacy Officer or General Counsel.

8.2.4 As specified in Paragraph 3.8 addressing the Family Educational Rights and Privacy Act, Contractor understands that it may have access to student educational records, under this Contract. MCCCD designates Contractor and its employees and/or agents as a school official for purposes of the Family Educational Rights and Privacy Act of 1974. Contractor shall safeguard those records and limit access to those records to only its employees and/or agents whose access to them is essential to the performance of this Contract. Contractor will not disclose those records without the prior written authorization of the student and/or the parent of a student who is a minor permitting MCCCD and Contractor to release the information according to the authorization.

8.2.5 At all times during this Contract, Contractor will maintain appropriate administrative, technical and physical safeguards to protect the security and privacy of the Confidential Information in use, in motion and at rest.

8.2.5.1 These safeguards include, but are not limited to, implementation of adequate privacy and security policies and data breach response plans that comply with industry standards and the requirements of applicable laws and the regulatory agencies responsible for enforcing them, as long as they meet or exceed MCCCD's information security and privacy policies and procedures as previously described herein. Contractor will supply the appropriate MCCCD representative with copies of those policies and plans upon request.

8.2.5.2 Contractor will maintain personnel policies that appropriately check the backgrounds of its employees who will be providing services to MCCCD. Contractor will supply the appropriate MCCCD representative with copies of those policies upon request.

8.2.6 Contractor will inform MCCCD's Chief Privacy Officer and the Office of General Counsel by sending an e-mail to protectprivacy@maricopa.edu immediately, and in no event later than within one (1) business day if Contractor and/or its contractors/agents has reason to believe that an actual or suspected security incident or any other circumstance has occurred in which MCCCD may be required to perform a risk assessment and/or provide a notification under applicable law, at which point MCCCD internal and/or external legal counsel will determine any additional information needed or steps to be taken, and will make a legal determination regarding its course of action. Any such notice will provide a description about the Confidential Information that was accessed as Contractor has available at the time of the notice. Contractor will keep the MCCCD Office of General Counsel updated

[2] See, e.g., **MCCCD Statement on Privacy** at https://chancellor.maricopa.edu/public-stewardship/governance/administrative-regulations/4-auxiliary-services/4.22-statement-on-privacy; **MCCCD Written Information Security Program** at https://chancellor.maricopa.edu/public-stewardship/governance/administrative-regulations/4-auxiliary-services/4.23-written-information-security-program; and **MCCCD Information Security Incident Response Plan** at https://chancellor.maricopa.edu/public-stewardship/governance/administrative-regulations/4-auxiliary-services/4.24-information-security-incident-response-plan.

promptly as additional details about the nature of the Confidential Information become available, and will communicate such information in a manner that maximizes the extent to which the attorney-client privilege and/or work product attaches to these communications. Furthermore, any such notice and all communications concerning a situation for which notice is provided are part of the confidential joint response of Customer and Contractor,

8.2.7 Contractor agrees to mitigate, to extent practicable, any harmful effect that is known to Contractor of a use or disclosure of Confidential Information in violation of this Contract by Contractor or its subcontractor.

8.2.8 For purposes of this Contract, "security incident" means the unauthorized access and/or misappropriation of Confidential Information. If in the event that applicable law requires notification to individuals or others of such a security incident or such incident places individuals at an actual risk of harm, Contractor will (i) be completely accountable and responsible, financially and otherwise, at no cost to MCCCD, (ii) provide assistance with the drafting and mailing of such notifications, (iii) retain a mutually agreed upon vendor to provide notification and call centering services, and (iv) offer to provide two (2) years of industry standard credit monitoring, identity theft restoration services and identity theft insurance to each affected individual at no cost to Customer or such affected individual. The requirement to offer such monitoring and insurance will only exist for individuals in those jurisdictions where such products are available.

8.2.9 If as result of the Contractor's systems, actions, and/or omissions, if a suspected or actual breach involving personally identifiable information or protected health information occurs, Contractor will obtain a mutually agreed upon vendor to provide at no cost to client forensic services, including, but not limited to, the collection of information in connection with a forensic and risk analysis. Contractor shall indemnify, defend and hold MCCCD, its agents, officers, officials, employees and volunteers harmless from and against all claims, damages, losses, and expenses (including but not limited to attorney fees and court costs) of any kind relating to the disclosure of personally identifiable information caused by the negligent or intentional acts or omissions of the Contractor, its agents, employees, or any tier of Contractor's subcontractors in the performance of this Amendment. Contractor will indemnify, defend and hold MCCCD harmless from claims of any kind relating to the disclosure of MCCCD Confidential Information caused by a possible or actual security infiltration or exfiltration involving technology of the Contractor, its agents, employees, or any tier of Contractor's subcontractors.

8.2.10 To the extent that Contractor transmits or processes Confidential Information outside of the United States, it agrees to comply with the data security and privacy laws of each country through which such information is transmitted or processed, as well as the data security and privacy laws of the jurisdictions of residence for the individuals whose data is used by Contractor.

8.2.11 If applicable, during the term of the Contract, Contractor will be required to promptly complete the Higher Education Cloud Vendor Assessment Tool (HECVAT) security assessment if it makes any revisions to its practices and policies that materially change its responses to that attachment.

8.2.12 If Contractor, its agents, employees, or any tier of Contractor's subcontractors in the performance of this Contract hosts or maintains MCCCD Confidential Information on its technology, Contractor warrants and confirms that the hosting or maintenance of that information meets applicable legal and industry security standards, including qualifying for "safe harbor" rules under applicable data breach laws.

8.3 RECORD AND DATA RETENTION, OWNERSHIP, ACCESS AND DECOMMISSIONING

8.3.1 As a political subdivision of the State of Arizona, MCCCD is subject to applicable laws related to the inspection and production of public records. A public record entails any record, either paper or electronic, made by a public officer (including members of the Governing Board, faculty, staff and administrators) and kept as a memorial of an official transaction. Pursuant to Arizona Revised Statutes §41-151.12, MCCCD must retain records according to established retention periods. Records required for ongoing or foreseeable official proceedings such as audits, lawsuits or investigations must be retained until released from such official proceedings. Thus, if applicable, the Contractor's hosted system shall have the ability to:

A. Archive records according to variable time periods/life cycles;
B. Search and retrieve records based upon content;
C. Place a litigation hold on records to ensure that they are not deleted;
D. Grant direct access to MCCCD for its own search and production of records;
E. Preserve meta data;
F. Produce electronic records in their native format; and
G. Comply with the Americans with Disabilities Act.

8.3.2 MCCCD owns all of the records and data of which Contractor has custody on MCCCD's behalf. Contractor will not disclose, use, destroy, transfer or otherwise manage those records and data except as provided in this Contract or, if the Contract is silent, without the express written approval of an authorized MCCCD representative. Contractor will work with MCCCD to transfer all of MCCCD's records and data to MCCCD on the termination or expiration of this Contract.

8.3.3 Contractor agrees to provide MCCCD access to records and Confidential Information that Contractor holds or uses on behalf of MCCCD upon written request of MCCCD with reasonable advance notice. Further, Contractor agrees to make amendments to Confidential Information as directed by MCCCD and will maintain a record of those changes.

8.3.4 Contractor agrees to maintain, and provide to MCCCD if requested, a record of when and to whom Confidential Information is disclosed.

8.3.5 MCCCD agrees to provide Contractor with adequate notice of any further limitations or restrictions on the use of Confidential Information, and modifications to the amendment of records or accounting of disclosures.

8.3.6 Confidential Information of the disclosing party will be returned to the disclosing party or securely destroyed promptly upon request of the disclosing party without retaining any

copies thereof, with any destruction confirmed in writing by receiving party, with any destruction confirmed in writing by receiving party, except to the extent copies are required by law to remain with Contractor.

8.4 MCCCD EXTERNAL ENTITY SECURITY AND HOSTING PRACTICES AND STANDARDS

This document identifies the security practices that are required for External Entities performing information technology services for MCCCD.

I. Definitions

The term “Authorized Visitor” means visitors who are pre-approved by MCCCD to access the Environments.

The term "Continental United States" refers to all of the United States on the North American continent. The Continental United States includes 49 states, i.e., each of the 50 states exclusive of Hawaii.

The term “External Entity” means the entity that is responsible for performing information technology services for MCCCD. External Entity is also comprised of various teams and individuals involved in information security at External Entity, including the executive-level oversight committee, corporate information, all lines of business (LoBs) and individual information security managers (“ISMs”) who are assigned by each LoB to represent the security leadership of each organization. Additionally, External Entity also includes any Subcontractor or third-party that External Entity deploys for the delivery of Services,

The term “Environment(s)” means MCCCD’s technology environments to which External Entity is granted access in order to provide the services.

The term “Service Location(s)” means External Entity offices from which the Environments may be accessed.

The term “Service(s)” means the information technology service(s) described and set forth under a written contractual agreement between MCCCD and External Entity.

The term “Subcontractors” means subcontractors retained by External Entity and its subsidiaries that assist in performing the Services.

II. Security Policies

External Entity’s corporate security policies must cover the management of security for both its internal operations as well as the Services External Entity provides to its customers, and apply to all External Entity employees, subcontractors and third-parties to External Entity, temporary employees, and individuals and legal persons that are involved in delivering services. These policies, which are aligned with the ISO/IEC 17799:2005 and ISO/IEC 27001:2005 standards, govern all areas of security applicable to the services.

Organizational Security
External Entity policy should describe the roles and responsibilities of various teams and individuals

involved in information security at External Entity, including the executive-level oversight committee, corporate information, all lines of business (LoBs) and individual ISMs who are assigned by each LoB to represent the security leadership of each organization.

The policy should also describe the principles for development, executive approval, implementation, and maintenance of all information security policies and practices at External Entity. This over-arching information security policy also describes governing principles such as 'need to know', least privilege, and segregation of duties.

- All individuals and legal persons who are involved in delivering Services are subject to External Entity security policies.

Asset Classification and Control

- External Entity policy should provide guidelines for all External Entity personnel regarding information classification schemes and minimum handling requirements associated with those classifications in an effort to ensure proper protection of External Entity and MCCCD information assets.

External Entity policy should require the implementation of anti-virus and personal firewall software and strongly recommends the use of Software Update Service (SUS) for Windows on desktop and laptop computers.

- External Entity policy should set requirements for use of the external entity corporate network, computer systems, telephony systems, messaging technologies, Internet access, and other company resources.

Human Resource Security

- External Entity should have a code of conduct that sets forth external entity's high standards for ethics and business conduct at every level of the company, and at every location where external entity does business throughout the world.
- The standards apply to employees, independent contractors, and temporary employees and cover the areas of legal and regulatory compliance and business conduct and relationships.
- Compliance-tracked training in ethics and business conduct and confidential information handling is required once every two years.

Physical and Environmental Security

- External Entity should have a policy that states corporate-level mandates for log retention, review, and analysis. Areas covered include minimum log requirements, responsibilities for the configuration and implementation of logging, alert review, problem management, retention, security and protection of logs, as well as compliance review.
- External Entity should have a policy that establishes guidelines for secure erasure of information, from all types of electronic and physical media, where use for current purposes is no longer needed and a decision has to be made regarding recycling or destruction. The policy is intended to protect external entity resources and information from security threats associated with the retrieval and recovery of information on electronic media.

Access Control

- External Entity should have a policy that describes logical access control requirements for all external entity systems, including authentication, authorization, access approval, provisioning, and revocation for employees and any other external entity-defined 'users' with access to

external entity systems which are not Internet facing publicly accessible systems.

- External Entity should have a policy that requires protection of information assets by external entity employees, through the use of strong password controls where passwords are being used as a method of authentication.
- External Entity's policy should describe the identity and access management method to define, allocate, adjust or remove an identity. The policy should address the characteristics of an identity, so as to ensure each identity is unique

Business Continuity Management

- External Entity should have a policy that addresses the requirements for the development, maintenance and testing of emergency response, disaster recovery, and business continuity practices to minimize the impact of business disruptive events on external entity's internal business operations globally.
- External Entity has a Business Continuity Plan that addresses MCCCD's business continuity requirements and this plan is tested at least once (1 time) every contract year

Compliance

- External Entity should have a policy that describes External Entity's treatment of data that resides on External Entity, MCCCD or third-party systems (including personally identifiable information or "PII") to which External Entity may be provided access in connection with the provision of the Services.
- External Entity must have a policy that requires reporting of and response to information security incidents in a timely and efficient manner. External Entity must also maintain a detailed incident response plan to provide specific guidance for personnel involved in or supporting incident response.
- External Entity must have a policy that provides requirements for External Entity employees to notify identified contacts internally, in the event of suspected unauthorized access to MCCCD data, PHI, PII and PCI.

III. Physical Security

Physical Security Safeguards: External Entity must maintain the following physical security standards, which are designed to prohibit unauthorized physical access at the Service Location(s).

- Physical access to Service Locations is limited to External Entity employees, Subcontractors and Authorized Visitors.
- External Entity employees, subcontractors and authorized visitors are issued identification cards that must be worn while on the premises.
- Authorized Visitors are required to sign a visitor's register, be escorted and/or observed when they are on the premises, and/or be bound by the terms of a confidentiality agreement with External Entity.
- External Entity security monitors the possession of keys/access cards and the ability to access Service Locations. Staff leaving External Entity's employment must return keys/cards and key/cards and all other access are deactivated upon termination.
- After-hours access to Service Locations is monitored and controlled by External Entity security.
- External Entity security authorizes all repairs and modifications to the physical security barriers or entry controls at Service Locations.

IV. Network Security

External Entity must take the following steps to secure access to the Environments:

- External Entity employs intrusion detection systems within the External Entity network to provide continuous surveillance for intercepting and responding to security events as they are identified. External Entity utilizes a network-based monitoring approach to detect attacks on open firewalls ports within External Entity's network. Events are analyzed using signature detection, which is a pattern matching of Environment settings and user activities against a database of known attacks. External Entity updates the signature database as new releases become available for commercial distribution. Alerts are forwarded to External Entity's IT department for review and response to potential threats.
- External Entity uses router rules, access control lists and segmentation on the External Entity network.
- External Entity's IT department manages and monitors all routers and firewall logs. Network devices are safeguarded via centralized authentication; usage is audited.
- When External Entity accesses the Environments residing on MCCCD's system over the Internet, it uses only (a) encrypted network traffic via industry standard Virtual Private Network (VPN) or equivalent technology, or (b) technology permitted by MCCCD's network administrator (e.g., direct dial-up or DSL if permitted on MCCCD's network). Unless otherwise specified in MCCCD's order, in (a) above, External Entity uses External Entity Continuous Connection Network (OCCN), which utilizes a persistent VPN tunnel and Cisco Software VPN Combination, for internet-based connections to the Environments.
- To the extent specified in MCCCD's order, External Entity may also use a desktop/laptop client based product when it accesses the Environments residing on MCCCD's system over the Internet. Examples include: Cisco Software VPN, Nortel Software VPN, Checkpoint Software VPN, Netscreen Software VPN, Point-To-Point Tunneling Protocol (PPTP), Neoteris Secure Sockets Layer (SSL) VPN, Aventail SSL VPN.
- External Entity shall ensure that all systems that contact MCCCD's network are controlled and managed from a virus protection perspective, to the extent that unmonitored or unwarranted systems (i.e. BYOD without External Entity Device Image) will be prohibited from connecting to MCCCD's network.

V. Data Management/Protection

Deletion of Environments: Upon termination of services or at MCCCD's request, External Entity will delete the Environments located on External Entity computers in a manner designed to ensure that they cannot reasonably be accessed or read, unless there is a legal obligation imposed on External Entity preventing it from deleting all or part of the Environments. Unless otherwise specified in writing, External Entity will archive Environments on tape for six months following termination of the services. MCCCD shall be entitled to request a recovery of such backed-up Environments within the six months following termination.

Reporting Security Incidents: If the MCCCD contract specifies that External Entity is required to access a production Environment to perform the Services and/or to receive production data into a development or test Environment to perform the Services, External Entity will take the following additional measures:

- External Entity will promptly evaluate and respond to incidents that create suspicions of unauthorized misappropriation of MCCCD's data. External Entity security will be informed of such incidents and, depending upon the nature of the activity, will define escalation paths and response teams to address the incidents.

- If External Entity determines that data in MCCCD's Environments has been misappropriated (including by a External Entity employee), External Entity will report such misappropriation to MCCCD in writing.
- External Entity personnel are instructed in addressing incidents where handling of data has been misappropriated, including prompt and reasonable reporting and escalation procedures.

Disclosure of Data: External Entity will not disclose data located on External Entity systems, including text and images, except in accordance with MCCCD's contract, MCCCD's instructions, or to the extent required by law. External Entity will use diligent efforts to inform MCCCD, to the extent permitted by law, of any request for such disclosure before disclosure is made.

Crisis Management and Escalation Management: External Entity policy will provide a detailed plan to address an identified infection or high-risk security breach (high-risk event). Such policy will include the detailed activities that address escalation of the resolution of the high risk event, up to an executive level crisis management.

VI. Access Control

Account Provisioning and Passwords: External Entity must maintain the following standards for provisioning access to and creating passwords for the Environments that are in the control of External Entity:

- Access is provisioned on a need-to-know basis.
- Passwords conform to the strong password guidelines that include complexity, expiration, duplicity and length. Passwords will not be written down or stored online unencrypted.
- Passwords are treated as External Entity confidential information.
- At MCCCD's request, External Entity will agree with MCCCD on a schedule for periodic password changes.
- User IDs and passwords to MCCCD's systems are not communicated to any other person without MCCCD's prior authorization.

General Access: In the event of employee terminations, deaths or resignations, External Entity will take immediate actions to terminate network, telephony and physical access for such former employees. External Entity security will periodically review accounts of terminated employees to verify that access has been terminated and that stale

VII. Additional External Entity Practices

Computer Virus Controls*:* External Entity must maintain the following computer virus controls for computers issued to External Entity employees:

- External Entity maintains a mechanism within the External Entity network that scans all email sent both to and from any External Entity recipient for malicious code and deletes email attachments that are infected with known malicious code prior to delivery.
- External Entity requires all External Entity employee laptops or other devices that can access MCCCD's network to be loaded with virus protection software. External Entity maintains mechanisms to ensure that virus definitions are regularly updated, and that updated definitions are published and communicated to employees and other device users. These mechanisms also give employees and other device users the ability to automatically download new definitions and update virus protection software. From time to time, External Entity security will conduct compliance reviews to ensure employees and other device users have the virus software

installed and up-to-date virus definitions on all desktops and laptops.

Information Security Managers: External Entity should have ISMs, who function as advocates within External Entity and carry the accountability to:

1. Ensure information security awareness to External Entity employees and management, and
2. Work collectively with that group to help implement and comply with External Entity's corporate security practices, policies and initiatives.

VIII. Human Resources Security

Personnel: All External Entity employees, independent contractors, and temporary employees must be required to abide by the External Entity code of ethics and by MCCCD rules, when visiting MCCCD sites. External Entity must place strong emphasis on reducing risks of human error, theft, fraud, and misuse of facilities. External Entity's efforts should include screening personnel, making personnel aware of security policies, and training employees to implement security policies. For example, employees are expected to have a clear understanding of password policies and policies concerning the handling of confidential information (in any form or shape).

Employee Security Requirements

External Entity employees must be required to take various measures to protect the security of the Environments. Employee obligations include written confidentiality agreements and compliance with company policies concerning protection of confidential information (e.g., External Entity code of conduct, acceptable use and information protection policies). Employees also are required to take the following measures to protect MCCCD's data:

- Store materials containing data securely and share those materials internally only for the purposes of providing the services.
- Dispose of paper copies of confidential materials and materials containing data in shredding bins designated for confidential information, and not in non-secure recycling bins or trashcans.

Subcontractors

- External Entity will obtain a written confidentiality agreement from each subcontractor before the subcontractor provides services. In addition, subcontractors that require access to MCCCD's Environments are required to sign a services provider agreement and a network access agreement. Included in the services provider agreement are the External Entity standards, which require the subcontractor to implement physical, technical and administrative safeguards consistent with External Entity's obligations under MCCCD's order and this document.
- External Entity is responsible for assuring that its subcontractors access, use, and protect the security of the Environments in a manner consistent with the terms of MCCCD's order and this document.

Employee Training

- All External Entity employees are required to complete information protection awareness training upon hiring and at least every two years thereafter. The course instructs employees on their obligations under the various central External Entity privacy and security policies. The course also trains employees on data privacy principles as well as data handling practices that may apply to their jobs at External Entity and are required by company policy, including those related to notice, consent, use, access, integrity, sharing, retention, security and disposal of

data.

- External Entity performs periodic compliance reviews to determine if employees have completed the online data privacy awareness-training course. If External Entity determines that an employee has not completed this training, the employee will be promptly notified and instructed to complete such training as soon as practicable, and may be subject to disciplinary action.
- External Entity promotes awareness of, and educates employees about, issues relating to security. External Entity prepares and distributes to its employees notices and other written material on security.

Enforcement

- External Entity must conduct security reviews, assessments, and audits periodically to confirm compliance with External Entity information security policies, procedures and practices. Employees who fail to comply with information security policies, procedures and practices may be subject to disciplinary action, up to and including termination.
- MCCCD will be entitled to audit External Entity's Security Policies every year, once per year.

VII. Additional External Entity Practices

Computer Virus Control*s:* External Entity must maintain the following computer virus controls for computers issued to External Entity employees:

- External Entity maintains a mechanism within the External Entity network that scans all email sent both to and from any External Entity recipient for malicious code and deletes email attachments that are infected with known malicious code prior to delivery.
- External Entity requires all External Entity employee laptops and other devices used to connect to the MCCCD network to be loaded with virus protection software. External Entity maintains mechanisms to ensure that virus definitions are regularly updated on all devices, and that updated definitions are published and distributed to employee devices. From time to time, External Entity Global Information Security will conduct compliance reviews to ensure employees have the virus software installed and up-to-date virus definitions on all desktops and laptops.

SAMPLE CYBERSECURITY CONTRACT TERMS

The following list provides examples of topics for security and privacy contractual terms that MCCCD External Entities may be asked to adopt; examples of sample verbiage are noted for some topics:

Background Check and other Personnel Policies

Contractor will maintain personnel policies that appropriately check the backgrounds of its employees who will be providing services to Customer in accordance with MCCCD policy. Contractor will supply the appropriate MCCCD representative with copies of those policies upon request.

Confidential Information

Sample Verbiage:

MCCCD information that is required to be kept confidential will be kept so in perpetuity.

For purposes of this Agreement, Confidential Information, including Customer Data, is defined as any and all Customer information and data whose collection, sharing, dissemination, use, preservation, disclosure, protection, storage, destruction and/or disposition is governed by federal, state, local and/or international law or regulation.

Personally identifiable information (e.g., social security numbers; an individual's full name in combination with their date of birth), personally identifiable education records, individually identifiable health information (e.g., an individual's name in combination with Health insurance subscriber identification number), and personally identifiable financial information and payment card information (e.g., financial account number, credit card number, and/or debit card number in combination with the required security code necessary to permit access) are examples of Confidential Information covered under the Arizona Revised Statutes (ARS), Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act of 1996 (HIPAA), Gramm–Leach–Bliley Act (GLBA aka Financial Services Modernization Act of 1999) and Payment Card Industry Data Security Standard (PCI DSS), respectively. In addition, Confidential Information includes data and other information that is proprietary to or developed by MCCCD such as institutional financial and performance records.

Confidential Information does not include (i) information the receiving Party already knows, (ii) information that becomes generally available to the public except as a result of disclosure by the receiving Party in violation of this Amendment, and (iii) information that becomes known to the receiving Party from a source other than the disclosing Party on a non-confidential basis, unless said source and the receiving party agree otherwise.

Contractor agrees that Confidential Information provided to it during the provision of service, or to which it may potentially have access, during the provision of service, shall be used only and exclusively to support the service and service execution and not for any other purpose. Such use shall not include examining data for targeted marketing either within the confines of the service or external to the service (e.g., keyword indexing).

i) The Contractor may use aggregate statistics on service usage in order to enhance or optimize the functionality of the service provided under the Master Agreement.

The receiving Party will limit access to Confidential Information to its employees who need to know the Confidential Information in order to carry out the activities under the Master Agreement and will instruct those employees to keep the information confidential. It is understood, however, that Contractor may disclose the Customer Confidential Information (including Customer Data) on a need to know basis to its agent(s) who are performing services, provided those agent(s) have executed confidentiality agreements and have agreed to materially the same or greater security and privacy obligations as Contractor provides with respect to Customer Data hereunder, and further provided that Contractor shall remain liable for any unauthorized disclosure of the Customer Confidential Information (including Customer Data) by those agent(s).

If a Contractor's staff person or Contractor's agent(s) potentially will have access to MCCCD's network, facilities, data, and/or Confidential Information, they may not perform any work involving such access until they have received MCCCD's privacy and security training, and/or accepted and agreed to adhere to MCCCD's privacy and security policies and procedures.[3] If exigent circumstances are presented, all or part of this requirement may be waived in writing by MCCCD's Chief Privacy Officer or General Counsel.

Contractor understands that it may have access to student educational records, under this Amendment. In accordance with the Family Educational Rights and Privacy Act of 1974 (FERPA), Contractor shall safeguard those records from improper disclosure and limit access to those records to only its employees and/or agent(s) whose access to them is essential to the performance of this Agreement. Furthermore, Contractor will not disclose those records without the prior written authorization of the student and/or the parent of a student who is a minor permitting MCCCD and Contractor to release the information according to the authorization.

At all times during this Agreement, Contractor will maintain appropriate administrative, technical and physical safeguards to protect the security and privacy of the Confidential Information in use, in motion and at rest. These safeguards include, but are not limited to, implementation of adequate privacy and security policies and data breach response plans that comply with industry standards and the requirements of applicable laws and the regulatory agencies responsible for enforcing them, as long as they:

I. Meet or exceed MCCCD's information security and privacy policies and procedures as described herein,

II. Do not conflict with MCCCD incident response requirements and, to the extent that they do, Contractor agrees to match and comply with MCCCD's requirements, and

III. Retain the level of protection provided for MCCCD's Confidential Information at a level that is materially the same or greater than the level of protection provided at the outset of the Term of this Agreement.

Contractor will supply the appropriate MCCCD representative with copies of those policies and plans upon request.

[3] See, e.g., **MCCCD Statement on Privacy** at https://chancellor.maricopa.edu/public-stewardship/governance/administrative-regulations/4-auxiliary-services/4.22-statement-on-privacy; **MCCCD Written Information Security Program** at https://chancellor.maricopa.edu/public-stewardship/governance/administrative-regulations/4-auxiliary-services/4.23-written-information-security-program; and **MCCCD Information Security Incident Response Plan** at https://chancellor.maricopa.edu/public-stewardship/governance/administrative-regulations/4-auxiliary-services/4.24-information-security-incident-response-plan.

Contractor will maintain personnel policies that appropriately check the backgrounds of its employees who will be providing services to Customer in accordance with MCCCD policy. Contractor will supply the appropriate MCCCD representative with copies of those policies upon request.

Contractor shall inform MCCCD's Chief Privacy Officer and MCCCD's Office of the General Counsel by sending an e-mail to protectprivacy@maricopa.edu immediately, and in no event later than within one (1) business day if Contractor's employee(s) and/or agent(s) have reason to believe that an actual or suspected security incident or any other circumstance has occurred in which MCCCD may be required to perform a risk assessment and/or provide a notification under applicable law, at which point MCCCD internal legal counsel will determine any additional information needed or steps to be taken, and will make a legal determination regarding its course of action. Any such notice will provide a description about the Confidential Information that was accessed as Contractor has available at the time of the notice. Contractor will promptly update the MCCCD Office of General Counsel as additional details about the nature of the Confidential Information become available, and will communicate in a manner that maximizes the extent to which the attorney-client privilege and/or work product attaches to these communications. Furthermore, any such notice and all communications concerning a situation for which notice is provided are part of the confidential joint response of MCCCD and Contractor,

Contractor agrees to mitigate, to the extent practicable, any harmful effect that is known to Contractor of a use or disclosure of Confidential Information in violation of this Amendment by Contractor–'s employee(s) and/or its agent(s).

For purposes of this Amendment, "security incident" means the unauthorized access and/or misappropriation of Confidential Information. If as a result of the Contractor's systems, actions, and/or omissions, a suspected or actual breach involving Confidential Information occurs and applicable law requires notification to individuals or others of such a security incident or such incident places individuals at an actual risk of harm, Contractor will (i) be completely accountable and responsible, financially and otherwise, at no cost to MCCCD, (ii) provide assistance with the drafting and mailing of such notifications, (iii) retain a mutually agreed upon entity to provide notification and call centering services, and (iv) offer to provide two (2) years of industry standard credit monitoring, identity theft restoration services and identity theft insurance to each affected individual at no cost to Customer or such affected individual. The requirement to offer such monitoring and insurance will only exist for individuals in those jurisdictions where such products are available.

MCCCD agrees that it will not provide Contractor with any data that contains payment card information.

If as a result of the Contractor's systems, actions, and/or omissions, a suspected or actual breach involving Confidential Information occurs, Contractor will obtain a mutually agreed upon entity to provide at no cost to MCCCD forensic services, including, but not limited to, the collection of information in connection with a forensic and risk analysis. Contractor shall indemnify, defend and hold MCCCD, its agents, officers, officials, employees and volunteers harmless from and against all claims, damages, losses, and expenses (including, but not limited, to attorney fees and court costs) of any kind relating to the disclosure of MCCCD Confidential Information caused by the negligent or intentional acts or omissions of the Contractor, its employees, and/or any tier of Contractor's agent(s) in the performance of the Agreement, as judicially determined by a court of competent jurisdiction. Contractor will indemnify, defend and hold MCCCD harmless from claims of any kind relating to the disclosure of MCCCD Confidential Information caused by a possible or actual security infiltration or exfiltration involving technology of the Contractor, its employees, and/or any tier of Contractor's agent(s), as judiciously determined by a court of competent jurisdiction.

To the extent that Contractor transmits or processes MCCCD Confidential Information outside of the United States, it agrees to comply with the data security and privacy laws of each country through which such information is transmitted or processed, as well as the data security and privacy laws of the jurisdictions of residence for the individuals whose data is used by Contractor.

During the Term of the Master Agreement, Contractor will be required to promptly update and resubmit complete the Higher Education Cloud Vendor Assessment Tool (HECVAT) security assessment, if it makes any revisions to its practices and policies that materially change its responses to that attachment. A copy of the version which Contractor last submitted on _____, 20__is attached hereto as Attachment __.

If Contractor, its employees, and/or any tier of Contractor's agent(s) in the performance of this Contract hosts or maintains MCCCD Confidential Information on its technology, Contractor warrants and confirms that the hosting or maintenance of that information meets applicable legal and industry security standards, including qualifying for "safe harbor" rules under applicable data breach laws.

If this Agreement involves the use by MCCCD of a site hosted or maintained by Contractor or should this Agreement involve the access by Contractor to MCCCD's site(s), Contractor shall use all reasonable endeavors to ensure no viruses or malicious code such as malware, spyware, key logger, bots (as the expressions are generally understood in the computing industry) are introduced, and that there is no corruption or modification or compromise of MCCCD systems or Confidential Information. Contractor agrees that it will not take any actions that will result in denial of service, interruption of service, outages, reduction or compromise in quality and efficiency of service, leakage or stealing of Confidential Information, interference with mandated lawful interception policy, methodology and provisions, enhanced risks of attacks, overbilling, frauds or any other compromise of the security of any and all data transmitted through the relevant systems and sites.

Cybersecurity Insurance

Dispute Resolution

Hosting Location

Maintenance and Incorporation of Privacy and Security Policies

Sample Verbiage:

"Agreement" means the Agreement, each annex and/or addenda added to the Agreement through an amendment, each Amendment to the Agreement, and the following Contractor documents ("Documents"), which are incorporated herein by this reference:

a) Certificate of Insurance
b) Business Resiliency Program Overview
c) Global Security Organization Overview
d) Hosting Services Executive Summary
e) Information Security Policy Statement
f) Information Security Program and Data Center Security Architecture Overview
g) Global Privacy Policy Statement
h) Incident Response Plan Executive Summary
i) Global Security Third-Party Security Risk Management

Mitigation of Effect of Security Incident

Notification of Security Incident

Sample Verbiage:

Contractor shall inform MCCCD's Chief Privacy Officer and MCCCD's Office of the General Counsel by sending an e-mail to protectprivacy@maricopa.edu immediately, and in no event later than within one (1) business day if Contractor's employee(s) and/or agent(s) have reason to believe that an actual or suspected security incident or any other circumstance has occurred in which MCCCD may be required to perform a risk assessment and/or provide a notification under applicable law, at which point MCCCD internal legal counsel will determine any additional information needed or steps to be taken, and will make a legal determination regarding its course of action. Any such notice will provide a description about the Confidential Information that was accessed as Contractor has available at the time of the notice. Contractor will promptly update the MCCCD Office of General Counsel as additional details about the nature of the Confidential Information become available, and will communicate in a manner that maximizes the extent to which the attorney-client privilege and/or work product attaches to these communications. Furthermore, any such notice and all communications concerning a situation for which notice is provided are part of the confidential joint response of MCCCD and Contractor,

Contractor agrees to mitigate, to the extent practicable, any harmful effect that is known to Contractor of a use or disclosure of Confidential Information in violation of this Amendment by Contractor–'s employee(s) and/or its agent(s).

For purposes of this Amendment, "security incident" means the unauthorized access and/or misappropriation of Confidential Information. If as a result of the Contractor's systems, actions, and/or omissions, a suspected or actual breach involving Confidential Information occurs and applicable law requires notification to individuals or others of such a security incident or such incident places individuals at an actual risk of harm, Contractor will (i) be completely accountable and responsible, financially and otherwise, at no cost to MCCCD, (ii) provide assistance with the drafting and mailing of such notifications, (iii) retain a mutually agreed upon entity to provide notification and call centering services, and (iv) offer to provide two (2) years of industry standard credit monitoring, identity theft restoration services and identity theft insurance to each affected individual at no cost to Customer or such affected individual. The requirement to offer such monitoring and insurance will only exist for individuals in those jurisdictions where such products are available.

Personnel Policies

Privacy Laws

Record and Data Retention, Ownership and Decommissioning

Sample Verbiage:

As a political subdivision of the state of Arizona, MCCCD is subject to applicable laws related to the inspection and production of public records. A public record entails any record, either paper or electronic, made by a public officer (including members of the Governing Board, faculty, staff and administrators) and kept as a memorial of an official transaction. Pursuant to Arizona Revised Statutes §41-151.12, MCCCD must retain records according to established retention periods. Records required for ongoing or foreseeable official proceedings such as audits, lawsuits or investigations must be retained until released from such official proceedings. Thus, if applicable, the Contractor's and/or its agent(s)' hosted system shall have the ability to:

a) Archive MCCCD records according to variable time periods/life cycles;
b) Search and retrieve MCCCD records based upon content;
c) Place a litigation hold on MCCCD records to ensure that they are not deleted;

d) Grant direct access to MCCCD for its own search and production of MCCCD records;
e) Preserve meta data;
f) Produce MCCCD electronic records; and
g) Comply with the Americans with Disabilities Act.

MCCCD owns all of the records and data of which Contractor has custody on MCCCD's behalf. Contractor shall not disclose, use, destroy, transfer or otherwise manage those records and data except as provided in this Agreement or, if this Agreement is silent, without the express written approval of an authorized MCCCD representative. Contractor shall work with MCCCD to transfer all of MCCCD's records and data to MCCCD on the termination or expiration of the Contract.

Contractor agrees to provide MCCCD access to records and Confidential Information that Contractor holds or uses on behalf of MCCCD upon written request of MCCCD with reasonable advance notice. Further, Contractor agrees to make amendments to Confidential Information as directed by MCCCD and will maintain a record of those changes.

Contractor agrees to maintain, and provide to MCCCD if requested, a record or when and to whom Confidential Information is disclosed.

MCCCD agrees to provide Contractor with adequate notice of any further limitations or restrictions on the use of Confidential Information, and modifications to the amendment of records or accounting of disclosures.

Confidential Information of the disclosing Party will be returned to the disclosing Party or securely destroyed promptly upon request of the disclosing Party without retaining any copies thereof, with any destruction confirmed in writing by receiving Party, except to the extent copies are required by law to remain with the receiving Party.

MCCCD shall maintain student information according to the retention schedule found at: https://chancellor.maricopa.edu/public-stewardship/records-information/records-retention-and-disposition-schedules-for .

Termination for Breach

GENERAL TERMS AND CONDITIONS

Any deviations to the General Terms and Conditions will NOT be considered in this proposal

These General Terms and Conditions, the other provisions of the RFP and amendments to it, the Proposer proposal, and MCCCD's purchase order terms ("Contract Documents") along with any engagement letter will constitute the provisions of the contract between MCCCD and successful Proposer ("Contract"). MCCCD reserves the right to negotiate with the successful Proposer and modify any of the provisions of the Contract upon mutual written agreement of the parties. The RFP, amendments to it, and MCCCD's purchase order terms will take precedence over any inconsistent terms in a proposal or other documents. The term "days" as used in this Contract means business days, unless otherwise specified.

9.1 PARTIES TO AGREEMENT

The Contract shall be between the MCCCD and the successful Proposer ("Contractor").

9.2 LIABILITY FOR TAXES

The Contractor is responsible for paying all taxes applicable to its operations, business property and income. MCCCD shall not be liable for any tax imposed either directly or indirectly upon the Contractor, except that MCCCD will pay as part of the Contract price any transaction privilege or use tax assessed on Contractor's provision of the services or materials under the Contract.

9.3 FORCE MAJEURE

If the performance of a party under this Contract is interrupted or suspended due to riots, war, public emergencies or calamities, fires, earthquakes, Acts of God, government restrictions, labor disturbances or strikes, or other condition beyond any control of that party ("Force Majeure"), performance by that party will be suspended for the reasonable duration of the Force Majeure. The party claiming that its performance is interrupted or prevented must promptly deliver notice to the other party identifying the Force Majeure and use its best efforts to perform to the extent that it is able. If the Force Majeure does not abate within a reasonable amount of time, then either party may terminate this Contract by providing written notice to the other party. Alternatively, the parties may agree to extend the term of the Contract for a period of time equal to the time equal to the Force Majeure.

9.4 CONTRACT ASSIGNMENT

Contractor may not, in part or in whole, subcontract (except as otherwise specified in Contractor's proposal to the RFP), delegate or assign this Contract without the prior written permission of a representative of MCCCD authorized to sign contracts.

9.5 NO WAIVER

MCCCD's failure to notify the Contractor or to object to the Contractor's non-compliance with the terms of the Contract shall not be deemed a waiver of MCCCD's right to demand compliance with the Contract or to terminate the Contract for breach for the Contractor's subsequent non-compliance with any term of the Contract, or its repeated failure to perform according to the Contract.

9.6 FINANCIAL TRANSACTIONS

If the Contractor is responsible for handling any type of financial transaction for MCCCD, the Contractor shall demonstrate annually, as applicable, that it complies with the Statement on Standards for Attestation Engagements (SSAE) No. 16, known as SSAE 16, established by the Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA). The Contractor shall provide its annual report, as applicable, on a reporting form or forms adopted as part of SSAE No. 16 no later than 30 days after MCCCD requests it in writing.

9.7 CONTRACT EXTENSION

Should the RFP provide options for extending the Contract beyond its initial term, MCCCD reserves the right to exercise those options without prior written notice and by the issuance of a purchase order or Procurement card to the Contractor. If the Contractor does not wish to renew the Contract, it must submit a written notice of its desire to cancel, which must be received by MCCCD's Purchasing Department no later than ninety (90) days prior to the end of the current term.

Notwithstanding that the Contractor has sent a notice of intent not to renew, MCCCD reserves the right to unilaterally extend the Contract for a period of sixty (60) days beyond the final option term of the contract should it be determined it is in the best interests of MCCCD to do so.

9.8 FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT

If Contractor has access to students' educational records, Contractor shall safeguard those records and limit its employees' and/or agents' access to the records to those persons for whom access is essential to the performance of this Contract. Contractor is prohibited from disclosing those records without the prior written authorization of the student and/or the parent of a student who is a minor permitting MCCCD and Contractor to release the information according to the authorization. At all times during this Contract, Contractor shall comply with the terms of the Family Educational Rights and Privacy Act of 1974 ("FERPA") in all respects and shall be responsible for ensuring that any subcontractors involved in the Contract work also comply.

1. MCCCD acknowledges that certain information about MCCCD's students is contained in records it maintains and that this information can be confidential by reason of the Family and Educational Rights and Privacy Act of 1974 (20 USC 1232g) and related Institution policies unless valid consent is obtained from MCCCD's students or their legal guardians, where applicable. Both parties agree to protect these records in accordance with FERPA and Institution policy. To the extent permitted by law, nothing contained herein shall be construed as precluding either party from releasing such information to the other so that each can perform its respective responsibilities. The MCCCD shall advise Contractor whenever any MCCCD's students have requested a privacy block, prohibiting release of FERPA protected information.
2. Contractor agrees that it may create, receive from or on behalf of MCCCD, or have access to, records or record systems that are subject to the Family Educational Rights and Privacy Act ("FERPA"), 20 USC 1232g (collectively, the "FERPA Records"). Contractor represents, warrants, and agrees that it will:
    a. hold the FERPA Records in strict confidence and will not use or disclose the FERPA Records except as
        i. permitted or required by this Agreement,
        ii. required by law, or
        iii. otherwise authorized by Institution in writing;
    b. safeguard the FERPA Records according to commercially reasonable administrative, physical and technical standards that are no less rigorous than the standards by which Contractor protects its own confidential information; and
    c. continually monitor its operations and take any action necessary to assure that the FERPA Records are safeguarded in accordance with the terms of this Agreement.
3. At the request of MCCCD, Contractor agrees to provide MCCCD with a written summary of the procedures Contractor uses to safeguard the FERPA Records.
4. For purposes of this Agreement, both Parties shall designate each other as a school official with a legitimate educational interest in the educational records of participating students to the extent that access to School's records is required to carry out the terms of this Agreement.

9.9 INDEMNIFICATION

To the fullest extent permitted by law, Contractor shall defend, indemnify, and hold harmless MCCCD, its agents, officers, officials, employees, and volunteers from and against all claims, damages, losses, and expenses (including but not limited to attorney fees and court costs) arising from breach of a material term of this Contract, or from the negligent or intentional acts or omissions of the Contractor, its agents, employees, or any tier of Contractor's subcontractors in the performance of the Contract. The amount and type of insurance coverage requirements set forth above will in no way be construed as limiting the scope of indemnification in this paragraph.

9.10 PERMITS

The Contractor shall be responsible for filing for, obtaining and paying for all required permits, licenses, and bonding to comply with pertinent municipal, county, State and Federal laws.

9.11 PROVISION OF SUPPLIES, MATERIALS AND LABOR

The Contractor shall furnish all supplies, equipment, and all management and labor necessary for the efficient and sound provision of the services or materials it supplies under this Contract, or in subsequent extensions or amendments.

9.12 CONFLICT OF INTEREST

Notice is given of Arizona Revised Statutes §38-511 under which MCCCD may cancel a contract without recourse for any conflict of interest described in that law.

See: http://www.azleg.gov/FormatDocument.asp?inDoc=/ars/38/00511.htm&Title=38&DocType=ARS

9.13 SAFEKEEPING OF RECORDS

Contractor shall keep in a safe place all financial and performance records and statements pertaining to this Contract for a period of three (3) years from the close of each term of the Contract.

9.14 AUDITS

Contractor shall make available during normal business hours and with advance notice from MCCCD all records pertaining to the Contract for purposes of audit by MCCCD staff or other public agencies having jurisdiction over or audit rights involving the expenditure of MCCCD funds.

9.15 UNAUTHORIZED COSTS OR COSTS OUTSIDE SCOPE OF AGREEMENT; TRAVEL

Costs or expenses of the Contractor relating to its performance of this Contract that are not included in the Contract price or are not authorized by the Contract are the sole responsibility of the Contractor and not of or reimbursable by MCCCD. If the Contract specifies that MCCCD will reimburse the Contractor a specific cost, Contractor may not charge MCCCD that cost without MCCCD approving a prior estimate of it. Additionally, MCCCD reimburses travel and related expenses only at the rate that it reimburses its employees.

9.16 NON-DISCRIMINATION

Contractor will comply with all applicable state and federal law, rules, regulations and executive orders governing equal employment opportunity, immigration, and nondiscrimination, including the Americans With Disabilities Act. If applicable, the parties will abide by the requirements of 41 CFR §§ 60-1.4(a), 60-300.5(a) and 60-741.5(a). These regulations prohibit discrimination against qualified individuals based on their status as protected veterans or individuals with disabilities, and prohibit discrimination against all individuals based on their race, color, religion, sex, age, or national origin. Moreover, these regulations require that covered prime contractors and subcontractors take affirmative action to employ and advance in employment individuals without regard to race, color, religion, sex, national original, protected veteran status or disability. MCCCD also prohibits discrimination on the basis of race, color, religion, sex, sexual orientation, gender identity, national origin, citizenship status (including document abuse), disability, veteran status or genetic information.

1. Contractor agrees to abide by the provisions of Title VI and VII of the Civil Rights Act of 1964 (42 USC 2000e) which prohibits discrimination against any employee or applicant for employment or any applicant or recipient of services, on the basis of race, color, and national origin (Title VI) and race, religion, color, or national origin, and gender (Title VII); and further agrees to abide by Executive Order No. 11246, as amended; 45 CFR 90 which prohibits discrimination on the basis of age; and Section 504 of the Rehabilitation Act of 1973, or the Americans with Disabilities Act of 1990 which prohibits discrimination on the basis of disabilities.
2. Contractor agrees that while interacting with Maricopa County Community College District employees and students, it will comply with Title IX of the Education Amendments of 1972 (20 USC 1681), which prohibits discrimination on the basis of sex in any federally funded education program or activity. Contractor must include this provision in every subcontract or purchase order relating to purchases by MCCCD to insure that the subcontractors and vendors are bound by this provision.
3. Contractor additionally agrees that it will cooperate with any investigation by MCCCD of a claimed violation of the above, to abide by any interim measures imposed during the course of an investigation and/or final measures imposed as a result of an investigation, and that its contract may be terminated without further recourse in the event of a finding of a violation by Contractor or its employees, subcontractors and related parties.

9.17 COMPLIANCE WITH IMMIGRATION LAWS; LEGAL WORKER'S ACT

The Contractor shall at all times comply with the Federal Immigration Reform and Control Act of 1986 (and by any subsequent amendments) and shall indemnify, hold harmless, and defend MCCCD from any and all costs or expenses whatsoever arising out of Contractor's noncompliance. To the extent applicable to this Contract under Arizona Revised Statutes § 41-4401, Contractor warrants on behalf of itself and its subcontractors that it verifies the employment eligibility through the e-verify program of any employee it hires and complies with federal immigration laws and regulations relating to their employees. The Contractor shall at all times comply with the Federal Immigration Reform and Control Act of 1986 (and by any subsequent amendments to it) and shall indemnify, hold harmless, and defend MCCCD from any and all costs or expenses whatsoever arising out of Contractor's compliance or noncompliance with that law. Additionally, Contractor agrees to abide by all applicable laws that apply to it and this Contract, including executive orders of the Governor of the State of Arizona.

9.18 CONTRACT TERMINATION

MCCCD may terminate this Contract for convenience by giving Contractor 15 days' written notice of termination. MCCCD may terminate this Contract for the failure of the Contractor to perform according to the Contract by giving the Contractor 10 days' written notice of the failure to comply. MCCCD may terminate this Contract immediately if the Contractor files for bankruptcy or receivership, or takes any actions relating to insolvency, such as an assignment for the benefit of creditors.

9.19 BREACH CURE; REPLACEMENT

The Contractor shall perform all requirements of the Contract in a manner consistent with the highest industry or professional standards. If MCCCD provides the Contractor with a 10-day written notice, Contractor must take immediate action to correct the deficiency identified in the notice. Contractor's failure to cure the deficiency within 10 days of receipt of the written notice will result in termination of the Contract. If, in MCCCD's sole discretion, the Contractor diligently pursues correction of the default and correction cannot be completed in 10 days, MCCCD may extend the time for curing the default by providing the Contractor with written notice of the extension before the end of the 10-day period. MCCCD is entitled to exercise all of its remedies under applicable law and in equity relating to Contractor's breach.

9.20 INTERPRETATION

The parties intend this Contract to express their complete and final agreement.

9.21 RISK

The Contractor assumes all risks due to any unfavorable conditions within its indirect or direct control except Force Majeure. Additionally, the Contractor assumes all risk for difficulties in the nature of the project or the work that the Contractor knew or should have known before entering submitting its proposal on which this Contract is based, under a scope of work issued under this Contract, or, if applicable, at the time of individual purchases under this Contract..

9.22 WORK TO BE PERFORMED BY OTHERS

MCCCD reserves the right to perform any and all services in-house or to utilize the services of other firms on unrelated projects.

9.23 PURCHASES OF OTHER PUBLIC ENTITIES

MCCCD has entered into Cooperative Purchasing Agreements with Arizona State University, Maricopa County, and other public entities. MCCCD is also an active member of the Strategic Alliance for Volume Expenditures (SAVE) Cooperative agreement. Under these Cooperative Purchasing Agreements and with the concurrence of the Contractor, other public entities that are members of these associations or any entity within MCCCD may purchase services or materials, as applicable, off of this Contract unless Contractor explicitly specified in its proposal that it did not want to make the Contract available other than to MCCCD. This provision applies only to contracts that are for the provision of services or supplies on an "as-needed" basis throughout the contract term, and not to contracts for specific projects or one-time purchase where the contract expires on the completion of the project or the purchase.

9.24 PAYMENT

MCCCD will pay for services or materials under the Contract after the Contractor has supplied them and only after the Contractor submits a detailed invoice referencing a purchase order or Procurement card, itemizing the services/deliverables or materials provided and specifying the dates that they were provided. MCCCD may request supporting documentation for an invoice. Where the Contractor is to provide services or materials over a period of time, such as for a project, MCCCD may agree to pay progress payments. If approved, progress payments will be paid in arrears and require that the Contractor submit the detailed invoice specified in this clause. MCCCD reserves the right to dispute an invoice or make partial payment based on the Contractor's failure to perform the Contractor's work according to the Contract, including for lack of timeliness or failure to provide deliverables. CONTRACTOR MAY NOT BEGIN WORK UNDER THE CONTRACT NOR WILL ANY PAYMENT BE MADE WITHOUT THE CONTRACTOR RECEIVING A SIGNED PURCHASE ORDER OR PROCUREMENT CARD FROM THE MCCCD PURCHASING DEPARTMENT.

9.25 BILLING

If MCCCD permits the Contractor to receive progress payments, Contractor may only invoice in increments of 30 days or more. The monthly billings should be submitted to the "BILL TO" address or "E MAIL" address shown on the purchase order.

9.26 ADVERTISING AND PROMOTION

The name or logos of the MCCCD or those of any of the colleges, skill centers, or programs under MCCCD's jurisdiction shall not be used by Contractor except as may be required to perform this Contract and only as approved under MCCCD's "Use of MCCCD Marks" regulation at:

http://www.maricopa.edu/publicstewardship/governance/adminregs/auxiliary/4_19.php

9.27 UNAVAILABILITY OF FUNDS

MCCCD may terminate this Agreement, without penalty, if its Governing Board fails to appropriate funds in subsequent fiscal years to support the specific program that is the subject of this Contract. MCCCD shall give Contractor prompt written notice after it knows that funding will not be available.

9.28 NO WAIVER OF SOVEREIGN IMMUNITY

Nothing in this Agreement shall be interpreted or construed to waive MCCCD's sovereign immunity under the laws of the State of Arizona.

9.29 APPLICABLE LAW

The laws of the State of Arizona apply to every aspect of this Contract.

9.30 PROPERTY RIGHTS

Except for pre-existing works of the Contractor or works of third parties for which Contractor has the permission to supply to MCCCD under this Contract, MCCCD shall, at all times, retain ownership in and the rights to any creative works, research data, reports, designs, recordings, graphical representations, or works of similar nature ("Works") to be developed and delivered under this Contract. Contractor agrees that the Works are "works for hire" and assigns all of the Contractor's right, title, and interest to MCCCD.

9.31 DOCUMENTATION OF ANALYSES TO SUPPORT FINDINGS, CONCLUSIONS AND RECOMMENDATIONS

To the extent that the work under the Contract requires the Contractor to make findings, conclusions or recommendations to MCCCD,, the Contractor shall retain during performance and provide to MCCCD detailed analyses relating to each of its findings, conclusions or recommendations, whether or not the analyses support or are inconsistent with the findings, conclusions or recommendations,. Unless specified in the subsequent Parts of this RFP, Contractor shall provide that documentation separately but at the same time that it presents its findings, conclusions and recommendations. MCCCD reserves the right to withhold or deduct payments otherwise due to Contractor if it fails to provide the detailed analyses. In some instances, Contractor may be directed to prepare its findings, conclusions and recommendations under the direction of the Office of the General Counsel. In those instances, Contractor will submit its findings, conclusions and recommendations in a manner that maximizes the extent to which attorney-client privilege and work product protections apply to such deliverables.

9.32 NOTICES

Notices to MCCCD under this Contract shall be made in writing, and sent via certified mail, return receipt requested, or any other commercially reasonable method by which MCCCD is required by the deliverer to acknowledge receipt to: Purchasing Manager, Maricopa Community Colleges, 2411 West 14th Street, Tempe, Arizona 85281-6942.

9.33 REVISIONS TO THE CONTRACT WORK OR PRICE

Contractor is on notice that the only MCCCD representatives who may authorize revisions to the Contract are employees at MCCCD's District Office who are authorized to sign contracts. Revisions include deletions of or additions to the work, alterations of performance time, or changes in pricing. Any revision must be reflected in a written amendment to the Contract that is signed by a representative of MCCCD authorized to sign contracts. The person requesting a revision in the Contract, whether it is the Contractor or an MCCCD employee, must provide the authorized MCCCD representative with documentation to support the requested change. It is the Contractor's responsibility to ensure that revisions of the Contract have been appropriately authorized before proceeding with the revised work.

For contracts renewing annually, excluding those for which Proposers are required to provide future year pricing in their Proposals, MCCCD may review a fully documented request for a price increase only after the Contract has been in effect for one (1) full year. Unless the Contractor's scope of work has increased at MCCCD's authorization, a price increase adjustment will only be considered at the time of a Contract extension and shall be a factor in the extension review process. The requested increase must be based upon a cost increase to the Contractor that was clearly unpredictable at the time of the offer and is directly correlated to the price of the particular product or service. MCCCD will determine whether the requested price increase or an alternate option is in its best interest.

9.34 GIFTS, GRATUITIES, UNRELATED COMPENSATION AND CONFLICTS OF INTEREST

In the interest of public stewardship, MCCCD holds its employees, officers, and vendors to high ethical standards. Arizona state law prohibits an MCCCD employee or officer from participating in any way in any MCCCD decision, contract, sale or purchase if he or she has received something of value from an outside party whose interests are involved in that MCCCD decision, contract, sale or purchase. Additionally, Arizona state law precludes any MCCCD employee or officer from obtaining compensation of any kind for performing his or her responsibilities other than the compensation provided by MCCCD. MCCCD also has adopted a regulation that prohibits any employee from accepting any cash, currency, item with a value of more than $50 (from a single source in a fiscal year), meal, beverage or cost of entertainment if it could be interpreted as an enticement to receive MCCCD business (whether or not paid for by a vendor or by a vendor's personal funds) or if there is an expectation of future financial benefit to the vendor. In keeping with these policies, Contractor certifies that neither it nor, if applicable, its subcontractors, suppliers, or distributors, has offered anything of value, and will not offer

anything of value so long as it does business with MCCCD, to an MCCCD employee or officer responsible for MCCCD decisions, contracts, sales or purchases that may benefit Contractor or its subcontractors, suppliers or distributors.

9.35 DISABILITY GUIDELINES

If applicable to the work of the Contractor under this Contract, Contractor warrants that it complies with Arizona and federal disabilities laws and regulations. Contractor warrants that the products or services to be provided under this Contract comply with the accessibility requirements of the Americans with Disabilities Act of 1990, as amended (42 U.S.C. §12101 et seq.) and its implementing regulations set forth at Title 28, Code of Federal Regulations, Parts 35 and 36, Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. §794d) and its implementing regulations set forth at Title 36, Code of Federal Regulations, Part 1194; and maintain, if applicable, Web Content Accessibility Guidelines 2.0 at Level AA (WCAG 2.0 AA). Contractor agrees to promptly respond to and resolve any complaint regarding accessibility of its products or services. Contractor must provide, on request, accessibility testing results and written documentation verifying accessibility. Contractor further agrees to indemnify and hold harmless MCCCD from any claims arising out of its failure to comply with the aforesaid requirements. Failure to comply with these requirements shall constitute a material breach and be grounds for termination of this Contract.

SIGNATURE PAGE

Pursuant to Arizona Revised Statutes 35-391.06 & 35.393.06, proposer certifies that it does not have a scrutinized business operation in either Sudan or Iran.

SIGNATURE _____

PRINTED NAME _____

TITLE _____

COMPANY _____

ADDRESS _____

CITY, STATE, ZIP _____

TELEPHONE _____ FAX NUMBER _____

E-MAIL _____

Is your firm a:

( ) Corporation* ( ) Partnership ( ) Individual ( ) Joint Venture

- If a corporation, answer the following:
  a) Where incorporated:_____
  b) Date incorporated:_____
  c) Have your Articles ever been suspended or revoked? ( ) Yes ( ) No

  If yes, when, for what reason, and when were they reinstated:

- Has your firm or its parent or subsidiaries ever been debarred or suspended from providing any goods or services to the Federal Government or other public entities?
  If yes, when, for what reason, and when were they reinstated:

ATTACHMENT A

BIDDER'S STATEMENT

Interested Bidders are asked to review and provide, as completely and accurately as possible, a written response on each applicable section below:

TYPE OF BUSINESS ORGANIZATION

Please check the appropriate box(es).

_____ The Bidder represents that it operates as:

_____ A CORPORATION incorporated under the laws of

the State of _____

_____ An INDIVIDUAL

_____ A PARTNERSHIP

_____ A NON-PROFIT ORGANIZATION

_____ A JOINT VENTURE

Federal Employer Identification Number: _____

PARENT COMPANY and IDENTIFYING DATA

A "parent" company, for the purposes of this provision, is one that owns or controls the activities and basic business policies of the Bidder. To own the Bidding company means that the "parent" company must own more than 50 percent of the voting rights in that company. A company may control a Bidder as a "parent" even though not meeting the requirements for such ownership if the "parent" company is able to formulate, determine or veto basic policy decisions of the Bidder through the use of dominant minority voting rights, use of proxy voting or otherwise.

The Bidder:

_____ IS _____ IS NOT owned or controlled by a "parent" company.

If the Bidder IS owned or controlled by a "parent" company, Bidder shall provide the name, address, phone and fax numbers, and Federal I.D. No. of the company.

ATTACHMENT A
BIDDER'S STATEMENT (continued)
BIDDER REFERENCES
Private Business Contracts

MCCCD requires a minimum of three (3) current and local references for which you are providing same or similar products and services specified herein. Please indicate below the businesses for which you have provided such during the past two (2) years:

1 Company Name: _____

Address: _____

Phone #: _____ Fax #: _____

Contact Person: _____

Contract Period: From: _____ To: _____

Describe Services: _____

2 Company Name: _____

Address: _____

Phone #: _____ Fax #: _____

Contact Person: _____

Contract Period: From: _____ To: _____

Describe Services: _____

3 Company Name: _____

Address: _____

Phone #: _____ Fax #: _____

Contact Person: _____

Contract Period: From: _____ To: _____

Describe Services: _____

ATTACHMENT A
BIDDER REFERENCES (continued)
Federal, State or Other Political Subdivision Contracts

MCCCD is also interested in speaking with public agencies or educational institutions for whom you have provided such products and services covered herein:

1 Company Name: _____
Address: _____
Phone #: _____ Fax #: _____
Contact Person: _____
Contract Period: From: _____ To: _____
Describe Services: _____

2 Company Name: _____
Address: _____
Phone #: _____ Fax #: _____
Contact Person: _____
Contract Period: From: _____ To: _____
Describe Services: _____

3 Company Name: _____
Address: _____
Phone #: _____ Fax #: _____
Contact Person: _____
Contract Period: From: _____ To: _____
Describe Services: _____

ATTACHMENT A
BIDDER'S STATEMENT (continued)
ADDITIONAL BUSINESS INFORMATION
Standard Business Hours

1 Days of week available for services: _____
2 Business hours of operation: _____
3 On-call/Emergency service hours: _____
Phone Number(s): _____
Web Address: _____
FAX Number: _____

General Information

4 Business License Number: _____
5 Number of years in business under current name: _____
6 Number of offices in the State of Arizona: _____
7 Business Classification (check applicable category)
Minority Owned Business (MBE) _____
Woman Owned Business (WBE) _____

Does your firm hold this certification from any other agencies or companies?
No: ____ Yes: ____ With Whom? _____

8 Name and address of office assigned to handle the MCCCD account:

_____

_____

_____

9 Account Manager Information:
Name: _____
Office Phone: _____
Cell: _____

10 Contractors License Number(s): TYPE _____ NUMBER _____

_____ _____

11 Do you ever sub-contract any of your services? NO _____
YES _____
If YES, which services?: _____

ATTACH ADDITIONAL SHEETS IF NECESSARY TO FURTHER DESCRIBE THE EXPERIENCE AND QUALIFICATIONS OF YOUR FIRM FOR PROVIDING THE PRODUCTS/SERVICES UNDER THE CONTRACT

Attachment B

Privacy/Information Security Inquiry

Answer the following questions:

1. Will your product, service or solution involve the processing, review, maintenance, retention, or use of MCCCD Confidential Information by you or any other outside party?

2. Will the product, service, or solution involve hosting by you, or any outside party, (i.e. off-site storage or cloud-based hosting by one or more non-MCCCD parties) of MCCCD Confidential Information?

3. Will you, or any outside party, need access to servers, systems, networks or have access to other manners of storing or displaying MCCCD Confidential Information (i.e. paper files and documentation, electronic spreadsheets etc.)?

4. Specify any data elements that will be shared with or accessed by any external (non-MCCCD) party for this contract.

Include <u>one</u> of the following audit reports as part of this attachment.

- SOC 2 Type 2 Audit
- HIPPAA Audit
- Department of Defense Certification and Accreditation
- Federal Information Security Management Act (FISMA) Audit
- Payment Card Industry Data Security Standard (PCI DSS) Audit
- Health Insurance Portability and Accountability Act (HIPAA) Audit
- Federal Risk and Authorization Management Program (FedRAMP) security compliance certification
- Other audit by an independent organization which evaluates and provides an opinion on the existence and effectiveness of the organization's information security controls

If your company does not have one of the above audits available you must fill out the HECVAT Lite assessment tool and include it as part of Attachment C.

NOTE: When responding to this section, clearly identify in your proposal response each paragraph number shown above and your response to that paragraph.

Attachment C

CHECKLIST FOR MCCCD CONTRACTOR
SECURITY AND HOSTING STANDARDS AND PRACTICES
2.0 Security Policies

The Higher Education Cloud Vendor Assessment Tool HECVAT is an Excel file and impractical to attach. Please use this link to access the form. Complete the form and attach to your submission:

https://library.educause.edu/resources/2020/4/higher-education-community-vendor-assessment-toolkit

MCCCD CONTRACTOR SECURITY AND HOSTING PRACTICES AND STANDARDS

[Applicable only for firms that may be hosting confidential MCCCD information on their systems]

1. **Information Security Program**.

1.1. Contractor will provide (and will cause its agents to provide) to MCCCD their respective security measures, safeguards, and procedures for review and verification by MCCCD of compliance with the terms of this Addendum and will confirm to MCCCD that sufficient measures have been taken by Contractor (and any agents) to prevent unauthorized access to and disclosure of Confidential Information. If at any time MCCCD believes in good faith that continuing performance under the Agreement poses a security risk to MCCCD or its data, network, or systems, MCCCD may immediately suspend its performance of any action or terminate the Agreement for cause, in either case without penalty or claim of breach.

1.2. At a minimum, Contractor's information security program shall implement and maintain the following safeguards:

1.2.1. Contractor will, at a minimum, (i) install and maintain a working firewall to protect data accessible via the Internet; (ii) keep security patches up to date; (iii) use and regularly update anti-virus software; (iv) restrict access to data on a "need to know" basis; (v) assign a unique ID to each person with computer access to data; (vi) not use vendor-supplied defaults for system passwords and other security parameters; (vii) track access to data and systems by unique ID; (viii) regularly test security systems and processes; (ix) maintain a policy that addresses information security for employees and contractors; and (x) restrict physical access to Confidential Information.

1.2.2. Monitoring of Systems. Contractor shall have adequate monitoring systems in place in order to prevent, detect, analyze and contain suspicious activity targeted at or associated with, directly or indirectly, Confidential Information and/or the systems, processes and technology associated with the storage, transmittal, or processing of Confidential Information. Contractor shall also follow a documented incident response policy that allows it to react and recover from any suspicious activity as well as meet the requirements of Section 2.5 of this Addendum.

1.2.3. Shipping of Confidential Information. Contractor shall ship Confidential Information via secured courier or a delivery mechanism that allows for tamper prevention and detection as well as accurate tracking of delivery status. Records containing Confidential Information in electronic format must be stored in a secure computer network satisfying the requirements of this Addendum, the adequacy of which Contractor will monitor to protect Confidential Information against emerging security threats, and which Contractor will enhance as necessary to address such threats.

1.2.4. Storage of Confidential Information on Storage Devices. Confidential Information cannot be stored electronically outside of Contractor's network environment unless the storage device (e.g., backup tape, laptop, memory stick, computer disk, etc.) is protected by Strong Cryptography technology that is free from publicly available vulnerabilities (i.e., compliant with NIST requirements and recommendations). For purposes of this Addendum, the term "Strong Cryptography" shall mean a cryptographic implementation and associated key management procedures compliant with, at minimum, NIST and PCI DSS requirements as applicable based upon the data type, sensitivity level, and communication mechanism of the data being encrypted, and is free from known and publicly available vulnerabilities.

1.3. Security Testing. Contractor agrees to have an independent third party security audit performed at least annually on all systems that directly and indirectly connect to Confidential Information. Contractor also agrees to conduct regular penetration testing and vulnerability scanning on all systems that directly and indirectly connect to Confidential Information. If any critical finding is identified, Contractor shall remediate the critical finding within thirty (30) days. Any critical finding not remediated within thirty (30) days must be immediately escalated to MCCCD. All other finding must be remediated within ninety (90) days. At MCCCD's request, Contractor shall promptly provide written
attestation that Security Tests have been conducted by a third party in the prior twelve months as well as a detailed list of open vulnerabilities and remediation plan(s) for all systems directly or indirectly connected to Confidential Information. Contractor shall designate one of its resources as a security liaison for MCCCD, who is available to discuss Security Tests, security findings, and other security concerns relevant to Contractor's Systems and Confidential Information at regular intervals.

1.4. Contractor will maintain personnel policies that appropriately check the backgrounds of its employees, contractors, or agents who will be providing services to MCCCD. Contractor will supply the appropriate MCCCD representative with copies of those policies upon request.

1.5. For purposes of the Agreement and Addendum, "Security Incident" means an event or (chain of events) that compromises (or is likely to compromise) the confidentiality, integrity, security, or availability of Confidential Information, or the hosted system, or violates (or potentially violates) Contractor's IT security policies or the standards or requirements of this Addendum.

2. **Incident Response and Management**.

2.1. Contractor shall maintain, update and document an Incident Management Process ("IMP Documentation"), and shall manage, document, review, investigate and resolve all Security Incidents in accordance with the Incident Management Process. Contractor will provide copies of IMP Documentation to MCCCD upon request and shall certify that the IMP Documentation has been reviewed annually and incident response tests have occurred.

2.2. Disciplinary Actions. Contractor shall have policies and processes in place to promptly identify violations of security controls including those set forth herein, by Contractor employees, contractors, subcontractors, agents, and/or vendors. Access to MCCCD Confidential Information by Contractor's employees, contractors, subcontractors, agents, and/or vendors beyond the performance of services related to this Agreement or by an employee not associated with the relevant project shall be deemed a Security Incident. Any personnel or parties so identified shall be subject to appropriate disciplinary action.

2.3. Security Incident Notification. Contractor shall report to MCCCD's Chief Privacy Officer or designated representative all known or suspected Security Incidents involving MCCCD's Confidential Information immediately upon becoming aware of such Security Incident. Any such report shall provide the following information: (i) date, time, nature and impact of the Security Incident; (ii) actions taken in immediate response to the incident by Contractor; (iii) Contractor's assessment of risk; (iv) a root cause analysis explaining why the incident occurred; (v) future remediation plan, including but not limited to corrective measures to be taken, evaluation of alternatives, next steps; and (vi) all other information regarding the Security Incident that MCCCD may request. Contractor is required to cooperate with MCCCD during any investigation of a Security Incident, including but not limited to any analysis as to whether such Security Incident resulted in a "data breach" or "security breach" under applicable state, international, or federal data breach law, and shall continue providing appropriate status report to MCCCD regarding the resolution of the Security Incident and prevention of future such Security Incidents until the Parties agree that the Security Incident has been resolved. Further, to the extent directed by MCCCD, Contractor shall engage, at Contractor's sole expense, technical experts approved by MCCCD to investigate and analyze the impact of the Security Incident and to provide the report of results and conclusions of such investigation to MCCCD. MCCCD may require that Contractor's accessing, processing, and/or storing of Confidential Information be suspended, connectivity with Contractor be terminated, or other appropriate action be taken pending resolution.

2.4. Reimbursement for Security Incident. Contractor shall promptly pay for or reimburse MCCCD for all costs incurred by MCCCD in connection with any Security Incident including, without limitation, the cost of providing required notifications, identity monitoring and restoration services, crisis communication costs, legal costs, technical expert costs and the amount of any monetary fines, assessments, damages, and/or penalties imposed on MCCCD by any court or governmental authority resulting therefrom, or imposed pursuant to any applicable contract or as part of a settlement of potential claim. Contractor will indemnify, defend, and hold MCCCD, its agents, officers, officials, employees, and volunteers harmless from and against all third party claims, damages, losses, and expenses (including, but not limited, to attorney fees and court costs) of any kind relating to a Security Incident caused by the acts or omissions of the

Contractor, its employees, or any tier of Contractor's agent(s) in the performance of services related to this Addendum. Further, Contractor shall not provide notice of any actual or reasonably suspected unauthorized access to, or disclosure of, Confidential Information to any third party (including, without limitation, any individual that is the subject of the applicable Confidential Information) unless Contractor receives MCCCD's written consent and direction to do so.

2.5. Contractor agrees to mitigate any harmful effect that is known to Contractor of a use or disclosure of Confidential Information in violation of this Addendum by Contractor or its subcontractor.

2.6. To the extent that Contractor receives MCCCD's written consent to access or process data outside of the United States and then transmits or processes Confidential Information outside of the United States, it agrees to comply with the data security and privacy laws of each country through which such information is transmitted or processed, as well as the data security and privacy laws of the jurisdictions of residence for the individuals whose data is used by Contractor.

2.7. Prior to the engagement, Contractor agrees to complete the Higher Education Cloud Vendor Assessment Tool (HECVAT) security assessment upon MCCCD's request. Contractor represents and warrants that all responses within its submission are accurate and truthfully represents the security practices of Contractor. If applicable, during the term of the Agreement, Contractor will be required to promptly update and resubmit the HECVAT if it makes any revisions to its practices and policies that materially change its responses to that attachment.

2.8. If Contractor, its agents, employees, or any tier of Contractor's subcontractors in the performance of the Agreement hosts or maintains MCCCD Confidential Information on its technology, (i) Contractor warrants and confirms that the hosting or maintenance of MCCCD's Confidential Information meets applicable legal and industry security standards, including qualifying for "privacy shield" rules under applicable data privacy laws, and (ii) Contractor will provide evidence of satisfactory assessment by a third party auditor of information security environment and controls on an annual basis during the term of the Agreement. MCCCD may audit Contractor's relevant control environment and security practices relevant to this Addendum if: (a) Contractor fails to provide sufficient evidence of compliance with this Addendum; (b) a Security Incident has occurred; (c) an audit is formally requested by a government regulator applicable to MCCCD, its business, or the services related to this Addendum; or (d) applicable law provides MCCCD with a direct audit right.