



MARICOPA COUNTY COMMUNITY COLLEGE DISTRICT

REQUEST FOR PROPOSAL #3476-6

Medical Benefits Network, FSA, & COBRA Claims Administrator

Proposal Due Date

March 2, 2021 (local time)

MARICOPA COUNTY COMMUNITY COLLEGE DISTRICT

RFP # 3476-6

Medical Benefits Network, FSA, & COBRA Claims Administrator

SCHEDULE OF EVENTS

ACTIVITY	DATE
Release RFP	January 7, 2021
Questions Due	January 28, 2021
Proposals Due	March 2, 2021
Possible Interviews (if needed)	Week of 4/12 or 19
Proposed Contract Award	July 1, 2021
Contract Start Date	January 1, 2022

Table of Contents

GENERAL	1
PROPOSAL INSTRUCTIONS	4
SCOPE OF WORK / PROPOSAL REQUIREMENTS	8
RESPONDENT QUESTIONNAIRE	188
EVALUATION CRITERIA.....	25
PRICING SCHEDULE	26
SPECIAL TERMS AND CONDITIONS	28
GENERAL TERMS AND CONDITIONS	45
SIGNATURE PAGE.....	53
ATTACHMENT A	54
ATTACHMENT B	58



ACKNOWLEDGMENT OF RECEIPT

RFP # 3476-6

Medical Benefits Network, FSA, & COBRA Claims
Administrator

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 Fax to MCCCCD Purchasing at (480) 731-8190 or 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 companies 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

The Maricopa County Community College District (MCCCD) is a system of 10 colleges, 2 skill centers and numerous education centers dedicated to meeting the needs of students and businesses of Maricopa County and beyond. Each of our community colleges is individually accredited, yet part of a larger system, the MCCCD.

Our colleges offer approximately 1,000 occupational programs (degrees and certificates), and 37 academic associate degrees, and a total of 10,254 courses. We have flexible course delivery which includes online, televised, traditional classroom, hybrid, mail, accelerated, evening, weekend and open-entry/open-exit choices.

A considerable amount of additional information about MCCCD is available on our Institutional Data website:

<https://www.maricopa.edu/about/institutional-data>

The 2019 MCCCD Public Dashboard is available here:

http://www.maricopa.edu/business/ir/Fact_Book_and_Card.php

We strongly encourage you to find out more about MCCCD by reviewing the information available from these sources.

1.2 MCCCD DISTRICT MAKE-UP

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 MCCCDC's operations. In addition to the loss of all funding from the State, MCCCDC 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 MCCCDC 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 MCCCDC 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 MCCCDC 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, MCCCDC 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 recommended that you review our 2017 – 2020 Strategic Commitments and detail in your proposal how leveraging a strategic partnership with your company can assist MCCCDC 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/MCCCDC%20Strategic%20Commitments%202017-2020%20-%20Nov%2015%2C%202016.pdf>

1.6 VALUE ADDED OFFERINGS:

MCCCDC 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 MCCCDC 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 MCCCDC 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.

MCCCDC 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

The purpose of this Request for Proposal is to select a qualified administrator to provide comprehensive medical claims administration and provider network services on behalf of MCCCCD's self-funded benefits plan, in addition to COBRA and Flexible Spending Account Administration services.

2.2 PROPOSAL QUESTIONS

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

Larry Woo, C.P.P.B
Sr. Procurement Analyst
(480) 731-8521 FAX (480) 731-8190
E-Mail: Larry.Woo@domail.maricopa.edu

Questions must be sent by mail or e-mail. Questions will only be accepted until January 28, 2021. 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 February 8, 2021.

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 with all tabs, attachments, etc. in the order listed in Section 3.6. Do not submit a proposal with the required sections/tabs separated into individual documents. All required items of the proposal should be submitted on a single PDF file with the exception of the security audit (SOCS II), which may be its own separate file.

The Proposal must be emailed to: larry.woo@domail.maricopa.edu. The official submittal time of record will be the time stamp from the MCCCCD email server. The email time stamp must read no later than 3:00 p.m., Tuesday, March 2, 2021. 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 a delay in its delivery. It is the Proposer's responsibility to submit your Proposal with enough lead-time to account for any delay. An email acknowledgement 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 # 3476-6, Medical Benefits Network, FSA, & COBRA Claims Administrator
Proposal Closing Date: March 2, 2021 Time: 3:00 p.m. (Local Time)**

Section Two: PROPOSAL INSTRUCTIONS

Rev 090817

NOTE: MCCCDC email restricts attachments over 25MB. If your Proposal file is larger than 25MB you will need to compress it or use a zip file program to reduce it down to an allowable size. The only exception to sending your proposal as the one PDF file requirement would be if you were not able to compress, or zip, your file size to the 25MB restriction. In that case you may divide your file into smaller file sizes in order to use multiple emails to submit it. Setting up a secure electronic drop box for MCCCDC to retrieve your file is also an acceptable method if you so choose.

Before submitting your proposal, make sure that you have read, understood and comply with Part IV – Proposal Requirements, Paragraph 3.3 – Deviations from RFP. Requested deviations will not be considered after the submission deadline.

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.

2.7 PROPOSER MODIFICATIONS TO PROPOSALS

Section Two: PROPOSAL INSTRUCTIONS

Rev 090817

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 MCCC. The MCCC will schedule the time and location for any presentations as requested. Oral presentations will be evaluated.

2.11 AWARD WITHOUT DISCUSSION

The MCCC 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 commence the resulting contract as soon as possible after evaluation of the proposals. A written Notice of Award with a specific contract start date will be made prior to commencement of performance. The start date listed on the letter will be made with the intent that all services are implemented and ready for claims to be processed starting on January 1, 2022. Any change to the completion timeline must be agreed upon in advance and in writing by MCCC.

2.13 MCCC 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 MCCC 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

Section Two: PROPOSAL INSTRUCTIONS

Rev 090817

The MCCCCD 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 MCCCCD'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 MCCCCD from obtaining the most advantageous proposal.

SCOPE OF WORK

The Scope of Work, as may be modified through negotiation and/or by written addendum issued by Maricopa County Community College District ("MCCCD"), will be made a part of the Agreement. Services will include comprehensive medical claims administration and network services.

The provider awarded the agreement is expected to provide medical benefits services administration, COBRA administration, FSA administration, claims adjudication, resolve claims disputes, timely data file feed transfers, management of claims appeals, electronic payment capabilities, open enrollment periods, and other relevant administrative services.

The Scope of Work includes management and oversight of medical claims administration and network services. The provider will perform or provide the following:

1. Assignment of a senior administrative representative within the claim office who is assigned to answer questions from MCCCD benefits supervisor or designated Human Resources Department staff regarding claims handling or reporting.
2. Assignment of a customer service team to answer inquiries on claims, services, coverages, or other inquiries from employees. Contractor will provide 24-hour service access for participants.
3. Handle all appeals (including self-funded) and notify claimant of decision.
4. Creating and maintaining claims files.
5. Discussing claims, where appropriate, with physicians and other providers of service.
6. Obtaining and furnishing information regarding coordination of benefits.
7. Ability to manage ACH and other electronic forms of payment.
8. Provide periodic on-site vendor fairs at each of the ten college campuses including on-site support for open enrollments and Medicare eligibility.
9. Provide COBRA administration.
10. Provide Flexible Spending Account (FSA) administration.

MCCCD will provide employee information pertinent to carry out services, any other relevant materials and data, documents, policies and procedures to the contract awardee.

PROPOSAL REQUIREMENTS

Paragraphs 3.1 & 3.2 below require specific, written responses or confirmations. To be considered for selection, respondents shall meet/provide the following requirements:

3.1 MINIMUM REQUIREMENTS

- 3.1.1 Must be licensed by the State the business is in, if services requested require such licensure.
- 3.1.2 Must provide a completed Pricing Schedule (Section 6) signed by an authorized company signatory.
- 3.1.3 Must have carefully read and understand all parts of the RFP and certified that the Proposal is made in accordance therewith.
- 3.1.4 Must submit written answers to the Respondent Questionnaire (Section 4). All answers must be in the order in which the questions were asked.
- 3.1.5 Must exhibit extensive experience in the field of the coverages/services being proposed.
- 3.1.6 Must currently administer claims for employers within the state of Arizona. Must provide adjudication and repricing for claims. Must also provide MCCCCD with an out-of-state medical provider network for all employees, including employees that work outside of Arizona.
- 3.1.7 Must submit a SOC 2 Type 2 audit report as part of your proposal response.
- 3.1.8 Must sign MCCCCD Data Security and Data Confidentiality Addendums (Attachment B), which are to be incorporated as special terms and conditions to this RFP.
- 3.1.9 Must meet the following:
 - Complete this form and include it with your response.
 - Indicate “yes” or “no” as to your organization’s ability to comply.
 - Contractor will be held accountable for accuracy/validity of all answers.

MANDATORY MINIMUM REQUIREMENTS	YES / NO
1. Proposal is submitted net of commissions.	
2. Agree to submit your renewal to the District (and/or its designated consulting firm) 6 months prior to the renewal date and understand that if this renewal deadline is not met, the District will not grant a rate increase for the subsequent plan year.	
3. The current level of MCCCCD’s benefits and eligibility policies are the minimum required. Richer benefits may be offered but will not receive additional credit in the evaluation phase as benefit levels in excess of the minimum required is not a primary criterion.	
4. Must propose a single bundled package including network access, claims administration, FSA, COBRA network access/claims administration.	
5. Agree that your Group Medical Benefits Proposal and pricing is not conditional on acceptance of any prescription drug coverage from you or any other prescription benefit manager.	

Section Three: SCOPE OF WORK / PROPOSAL REQUIREMENTS

Rev 022718

6. Agree that your Group Medical Benefits Proposal and pricing is not conditional on acceptance of any behavioral health coverage from you or any other behavioral health vendor.	
7. Agree that your Group Medical Benefits Proposal and pricing is not contingent on acceptance of any stop-loss coverage for you or any other stop-loss vendor.	
8. The TPA must have at least 200,000 members with a minimum of 50,000 members in Arizona.	
9. Vendor has an office located within Maricopa County that will be servicing MCCCCD.	
10. Vendor must demonstrate its ability to comply with each requirement of this RFP. Its proposal must describe its security safeguards for both the transition and operating phases of the contract.	
11. Vendor must encrypt personally identifiable information and personal health information, including in transmission, at rest, and in storage.	
12. Vendor must demonstrate its compliance to maintain cyber insurance at levels that MCCCCD approves covering data privacy, security, and breach.	

Proposers who do not reply “YES” to all 12 items directly above will be eliminated without further consideration

3.2 SPECIFIC REQUIREMENTS

- Complete this form and include it with your response.
- Indicate “yes” or “no” as to your organization’s ability to meet the specific requirements.
- Vendor will be held accountable for accuracy/validity of all answers.

SPECIFIC REQUIREMENTS	YES / NO
1. Contract has a length of one (1) year with the option to renew for at least four (4) additional years.	
2. Contract includes an indemnification/hold harmless clause to protect the District.	
3. You agree to work with MCCCCD staff as the contract is being implemented and throughout the contract to secure Confidential Information provided to you under this Contract.	
4. The rates quoted in your proposal are firm and will not be recalculated based on actual enrollment.	

Section Three: SCOPE OF WORK / PROPOSAL REQUIREMENTS

Rev 022718

5. You agree that any early termination provision contained in your contract cannot be tied to the renewal or incur penalties.		
6. You agree that the District can terminate the contract for convenience at any time without cause provided a 30 day notice.		
7. If you answered "No" to any of the questions above, please provide an explanation below:		
Requirement No.	Explanation	

3.2.1 Claim Payment Procedures and Deadlines/Designated Claims Unit/Claim Management

3.2.1.1 Claims must be paid by the insurer in a timely manner. To facilitate timely payment, the Contractor is to take the following steps:

- A. Provide claim-processing instructions, which are clear and complete.
- B. Clearly state the mailing address for claims on the forms. Preaddressed claim envelopes for claim submission are optional. If envelopes are provided, the address need not be printed on the forms.
- C. When a claim has been denied, or paid in part, and the insured has filed an appeal, a response to the appeal will be issued no later than 60 days after the necessary information is provided for the appeal to be considered. "Necessary information" may include the insured's physician's input but may not include "peer review." When the file is complete, peer review and determination must be rendered within 60 days. A much shorter response time is desired.
- D. Payment of a claim means the actual preparation and mailing of the amount due the insured or the provider.

3.2.1.2 The Contractor's claim payment system will contain, at minimum, the following data and system edits to assure proper determination of eligibility and availability of data required by MCCCD:

- A. Identify Employees:
 - Participant names
 - Employee I.D. #
 - Date of birth
 - Coverage level

Section Three: SCOPE OF WORK / PROPOSAL REQUIREMENTS

Rev 022718

- Social Security numbers
- Health Insurance Claim Numbers (HICN's)
- B. Employee's dependent coverage election, effective dates - start and end dates - of eligibility, for employees and dependents.
- C. Employee claim or dependent claim.
- D. Claim incurred date.
- E. Claim paid date.
- F. Ability to work electronically with other vendors that support MCCCC.
- G. Electronic payment capabilities for timely payment processing.
- H. Identify disabled dependents and disabled employees.
- I. Identify full-time students and disabled students.
- J. Identify pooled/combined coverage (both spouses are employees and have children/family coverage equivalent).
- K. Identify domestic partner coverage including domestic partner dependents.

3.2.1.3 The Contractor shall make personnel available to any MCCCCD officer or employee for consultation on matters regarding this program. The Contractor shall honor the right of the policyholder to question the company in any case where the employee's rights under the contract are in question.

3.2.1.4 The Contractor will recover any overpayments of \$20 or more.

3.2.1.5 The Contractor will be required to update coverage records upon receipt of the monthly listings of covered employees, noting additions, changes and deletions. The Contractor will also be required update coverage records upon receipt of corrections of information printed on the weekly computer reports provided to the Contractor/Proposer by MCCCCD or by a TPA/Subcontractor of MCCCCD. The Contractor must be able to accept and update MCCCCD coverage records via electronic file transfer, HIPAA Compliant 834/5010A Format. The Contractor is responsible for receiving and verifying enrollment data. The Contractor must be able to modify and/or customize the information management system to receive and interpret data files provided by MCCCCD.

3.2.1.6 It is preferred that the Contractor maintain a claim paying facility within Maricopa County, but the Contractor may provide a toll-free telephone service to a facility located outside of the County. Set up of an 800 number by policy effective date is preferred; however, collect calls may be accepted by the Contractor.

3.2.2 Reporting Requirements

Vendor will be required to provide, at a minimum, the following reports for MCCCCD:

- A. Claim reports (monthly).
- B. Large claim reports (50% notification) (monthly).

Section Three: SCOPE OF WORK / PROPOSAL REQUIREMENTS

Rev 022718

- C. In-network vs. out-of-network utilization, including network savings recap (quarterly).
- D. Report on case/disease management (quarterly).
- E. Utilization summary including EE/DEP claims, in-network vs. out-of-network, out-patient vs. in-patient, top diagnoses and comparison to carrier norms, etc. (semi-annually).
- F. Report on ALL medical claim history for plan year(s) (annual).

3.2.3 Demonstrations

Qualified Proposers may be requested to provide a tour of any administrative or service facilities intended to provide benefits stated in the proposal. Such a tour may include demonstrations of technical capabilities for record keeping, claim payment, etc., as well as interviews with staff intended to serve MCCCCD.

3.2.4 Administering the Medical Plan

The administrative services to be provided to MCCCCD's medical benefit plan shall include, but not be limited to, the following:

- A. Providing and updating all required HIPAA Certificates and SBC's to employees.
- B. Creating and maintaining claims files.
- C. Evaluating claims to determine if they have been properly filed and advising claimants in meeting the requirements for additional information and proper completion of claim forms.
- D. Computing the benefits due in accordance with the current benefit plan document and/or documentation.
- E. Issuing drafts to the person or assignee entitled thereto.
- F. Discussing claims, where appropriate, with physicians and other providers of service.
- G. Obtaining and furnishing information regarding coordination of benefits.
- H. Applying claims control procedures necessary for the effective administration of the Plan.
- I. Reconciliation of issued and cleared checks.
- J. Investigating claims in which the charges appear higher than reasonable and customary.
- K. Preparing, printing and distributing the claim forms and other administrative forms required for the successful operation of the Plan.
- L. Notifying claimants of rejected claims and the specific reason or reasons for the rejection.

Section Three: SCOPE OF WORK / PROPOSAL REQUIREMENTS

Rev 022718

- M. Timely notification to claimants and MCCCCD of delayed claim payments that are caused by the presence of duplicate coverage or an error of omission in claim payment documentation.
- N. Verifying eligibility to a provider of service. TPA/vendor must have web eligibility verification available to providers to utilize after hours of operation.
- O. Establishment of quality assurance standards and control mechanisms for assurance of compliance with such standards.
- P. Print checks or drafts and corresponding explanation of benefits.
- Q. Respond within one working day to any inquiry from MCCCCD benefits supervisor or designated Human Resources Department staff regarding the disposition of a pending claim.
- R. Assignment of a senior administrative representative within the claim office who is assigned to answer questions from MCCCCD benefits supervisor or designated Human Resources Department staff regarding claims handling or reporting.
- S. Assignment of a customer service team to answer inquiries on claims, services, coverages, or other inquiries from employees. Contractor will provide 24-hour service access for participants.
- T. Handle all appeals (including self-funded) and notify claimant of decision.
- U. Preparation and distribution of ID Cards to the District's participants within thirty days of enrollment.
- V. Provide adequate hospital data to the District's auditor, and state and federal auditors, when requested.
- W. Ability to manage ACH and other electronic forms of payment.
- X. Provide periodic on-site vendor fairs at each of the ten college campuses including on-site support for open enrollments and Medicare eligibility.
- Y. Provide COBRA administration.
- Z. Provide Flexible Spending Account (FSA) administration.

3.2.5 Enrollment

MCCCCD reserves the right to declare multiple open enrollment periods per contract period, to take place prior to the contract effective date.

3.2.6 Denial of Eligibility

The contracting company will not deny any eligible person benefits to which otherwise entitled under the plan, due to the error or omission of MCCCCD.

3.2.7 Implementation Requirements

To properly implement the policy by the effective date, January 1, 2022, the successful company will be required to devote staff attention to the following implementation activities:

Section Three: SCOPE OF WORK / PROPOSAL REQUIREMENTS

Rev 022718

- A. Revision of specimen policy boilerplate to conform to specifications.
- B. Provision of documents required in these specifications by October 1, 2021.
- C. Provide a sufficient quantity of open enrollment materials by October 1, 2021.
- D. Preparation of employee booklets. Draft to be presented to MCCCDC for approval by October 1, 2021. Printing and delivery to MCCCDC no later than November 15, 2021, in sufficient quantities for all employees currently covered, plus 20% additional. Additional supplies of booklets may be provided later, if requested by MCCCDC.
- E. Explanation of benefits and procedures to employee groups. The Contractor may be required to provide a representative to attend group transition sessions for employees. Such sessions would be scheduled in Maricopa County at varied sites. The representative would, at the request of MCCCDC, answer questions and/or make a brief presentation.
- F. Claim forms and instructions. Sufficient initial supplies of claim forms and instructions for all benefits must be supplied by November 15, 2021. MCCCDC will assist in distribution of supplies to various employee locations.
- G. Enrollment/eligibility data. The Contractor must accept MCCCDC transfer files, which identify eligible employees and dependents. The carrier must be able to provide through a computerized format the ability to reconcile participant's eligibility in the monthly billings and quarterly audits. The reconciliation and audit function need to be performed by the carrier. MCCCDC is able to provide the data via data transfer or Excel/dat file. The contractor reports must be provided to MCCCDC in Excel/dat format no later than twelve weeks before enrollment. The Contractor must be able to transfer eligibility /enrollment information to other health vendors including but not limited to PBM, EAP, and dental.
- H. All enrollment/communication materials sent to employees will be via first class mail, unless another mail class is authorized by MCCCDC.
- I. The Contractor will provide and pay for all enrollment forms, claims forms and checks, certificates of insurance, employee booklets, identification cards, announcement forms and any other forms required for proper administration of coverage.
- J. Identification cards must be supplied within seven days of provision of the eligibility list or enrollment forms for all covered employees. For employees with family coverage, a minimum of two cards is to be provided. **The TPA must also print and make available by December 1st notice to all employees on how to procure care. The carrier will assist in the preparation and distribution of such a notice and in the distribution of notification cards.**
- K. Files must be sent/received utilizing acceptable electronic security measures. E-mail notifications should be sent to employees confirming any changes to passwords for all websites.

Section Three: SCOPE OF WORK / PROPOSAL REQUIREMENTS

Rev 022718

3.2.8 Commissions

No commissions will be payable.

3.2.9 Evidence of Insurability

No evidence of insurability will be required except in the case of late enrollment or as specified in the proposed plan of benefits for medical insurance.

3.2.10 Installation

The claims administrator will be responsible for drafting of the insurance contract, summary plan descriptions (booklets), and will print all booklets. Cover artwork and paper stock should match that used by "MCCCD brochures". MCCCD will provide camera-ready artwork for covers. All such materials will be subject to review and modification by MCCCD. The claims administrator will prepare and print medical identification cards for distribution to covered employees. It is preferred that employee identification numbers issued by MCCCD be used as the identification number. The claims administrator will assist MCCCD in the enrollment processes. Information meetings will occur at all campuses during the open enrollment sessions scheduled by MCCCD. Annual enrollment is an online process for employees.

3.2.11 MCCCD Contributions

MCCCD reserves the right to change their subsidy of the flexible benefits program for employees.

3.2.12 No Gain/No Loss

Takeover will be on a no-loss, no-gain basis; that is, no individual will lose coverage solely on the basis of a change in carrier. The "actively at work provision" will be waived for plan participants covered on December 31, 2021 for benefits by the District.

3.2.13 Renewals

Renewal quotations will be required 6 months prior to the end of the policy year (i.e., January 1).

3.2.14 Coordination

The Contractor must be able to coordinate benefits/enrollment with the District's other vendors; including PBM and EAP.

3.3 DEVIATIONS FROM RFP

Proposers must specifically provide a separate listing of 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

Section Three: SCOPE OF WORK / PROPOSAL REQUIREMENTS

Rev 022718

discretion. The Proposer in choosing the respond to this RFP, must demonstrate in its Proposal that it accepts the terms upon which the MCCCCD 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 MCCCCD 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.

3.4 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.

3.5 AWARD CONSIDERATION

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

3.6 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
- Tab 6: Warranty (if required)
- Tab 7: Signed Addenda Acknowledgement (if any)
- Tab 8: Deviation to Terms and Conditions (if any)
- Tab 9: Attachment B-Signed MCCCCD Data Security and Data Privacy Addendums
- Tab 10: SOC 2 Type 2 security audit report (may be included as a separate PDF file)

RESPONDENT QUESTIONNAIRE

Respond to each item completely and in the order shown. Clear reference to readily accessible back-up material (e.g., plan documents, reports, charts, etc.) is acceptable. Incomplete or inaccurate answers will result in the loss of points in the evaluation scoring process. Failure to provide required information may cause the proposal to be deemed non-responsive.

4.1 GENERAL QUESTIONS

- 4.1.1 What is the full legal name of your company?
- 4.1.2 Provide references of three current clients of similar size for the same product(s).
- 4.1.3 Provide references of three former clients of similar size for the same product(s).
- 4.1.4 Will you provide the benefit schedules exactly as described? If not, please explain the changes you would require and the reasons for them.
- 4.1.5 Will you allow a 60-day grace period for unpaid premium/fees?

4.2 ACCOUNT MANAGEMENT

- 4.2.1 Provide a detailed project plan that includes the following:
 - Implementation Process
 - Assigned Team
 - Responsibilities of each team member
 - Resumes on each team member
 - Identify the person(s) who will be responsible for tracking and reporting full-time student status
 - Calendar of dates in table form for completion of each activity
 - Identify critical dates
- 4.2.2 What location/office would be responsible for providing account management to MCCCCD?
- 4.2.3 Provide a list and detailed description (including frequency) of report provided on a standard basis at no additional cost to your clients.
- 4.2.4 Provide a list and detailed description of special reports available for additional costs (include applicable costs for each).

4.3 MEDICAL PLAN CLAIM ADMINISTRATION

- 4.3.1 Will you administer the PPO plan as described in this RFP? If not, please explain the changes you would require and the reasons for them. Describe in detail any significant exclusions from coverage (i.e., organ transplants, etc.).

Section Four: RESPONDENT QUESTIONNAIRE

Rev 022718

- 4.3.2 From what office would routine administration and claims be handled? Are there any plans to move or close this office? How many group medical plans and claims does this office process annually?
- 4.3.3 Do you plan any revisions in your claims systems or systems hardware? If so, when and to what extent?
- 4.3.4 Describe how you will handle claims incorrectly submitted to you for services rendered prior to the effective date.
- 4.3.5 List the tools (i.e., unbundling, software, etc.) used to assure that claims are being processed accurately.
- 4.3.6 How long do you pend claims awaiting additional provider information?
- 4.3.7 Will you administer "coordination of benefits" as described in the District's plan document?
- 4.3.8 Describe your procedure for auditing hospital bills. If payment is DRG based, what is your procedure for validating DRG coding.
- 4.3.9 Describe your guideline with respect to detection of and action on overcharges, excessive hospital confinements, unnecessary hospitalization and other medical treatments or procedures, repeaters and other cost control programs you may utilize.
- 4.3.10 Describe your procedures for detecting duplicate payments and recovering such amount from providers and employees.
- 4.3.11 Explain your procedures for handling claim inquiries from employees? From MCCCCD?
- 4.3.12 Are you willing to provide documentation of all case specific internal audit results to the District? If so, how often will this information be made available?
- 4.3.13 State your definition of a claim transaction. Based on the definition, what has been your average in house service time, expressed in business days, for processing a transaction during the last three months?
- 4.3.14 Do you have a methodology in place to establish a maximum allowable charge on out-of-network charges? If yes, what is that methodology? Is this methodology negotiable?
- 4.3.15 Do you provide a service delivery guarantee with cost reimbursement?
- 4.3.16 Describe the utilization review process in place for out-of-network claims and the mechanisms in effect to steer out-of-network users into the network when significant medical episodes are foreseen.
- 4.3.17 Please provide samples of the following:

All statistical claim studies available (with an indication of the frequency, cost and timeliness of such studies) including but not limited to:

Report	Frequency	Available Online (Y/N)
a) Savings analysis of claim payment reductions due to negotiated payments as it relates to geographic averages, coordination of benefits, employee copayments and ineligible charges.	Monthly	

Section Four: RESPONDENT QUESTIONNAIRE

b)	Listing of aggregate claims payments.	Monthly	
c)	Claims by sub-line, i.e., hospital outpatient, surgery, physician, etc.	Monthly	
d)	Listing of any individual claims in excess of \$10,000 per calendar year.	Monthly	
e)	Analysis of utilization patterns in fee-for-service health care	Monthly	
f)	Report Showing In-Network vs. Out-Of-Network Utilization	Monthly	
g)	Report showing claims paid by each College, District office separately	Monthly	
h)	Report showing all entities combined in (g) above	Monthly	

4.3.18 Is pre-admission certification and concurrent review provided by an outside vendor, delegated, or performed in-house? If outsourced, identify vendor by name.

4.3.19 Provide copies of management reports related to the below listed items. Hospitalization requests, approvals and denials by:

- Diagnosis (both primary and secondary).
- Medical/surgical admissions.
- Employee/dependent.
- Bed days requested, authorized, reduced, etc.
- Analysis of results and cost savings.

Are the management reports available online?

4.3.20 Describe all other services that are available to the District's staff online.

4.3.21 Describe your preparedness plan for a breach of security.

4.3.22 Please indicate your willingness to pay for mistakes made by your organization. For example, if ID cards are printed in error and the error was clearly your fault, are you willing to pay for the reprint of cards?

4.4 MEDICAL CLAIMS ADMINISTRATION

4.4.1 Indicate all provider networks you are approved to work with

4.4.2 Do your services include full claim fiduciary services (providing claims level appeals both level 1 and 2)? The District is currently not involved in the appeals process.

4.4.3 Indicate all provider networks you are approved to work with.

4.4.4 Provide your performance statistic for the last 12 months for all of the following:

Claims Turnaround time:

Percentage within 14 calendar days

Percentage within 30 calendar days

Section Four: RESPONDENT QUESTIONNAIRE

Rev 022718

Claims Financial Accuracy:

Percentage paid accurately

Call Center Answer Speed:

Percentage of calls answered within 30 seconds

Problem Resolution:

Percentage of caller issues solved during initial call

- 4.4.5 Provide a summary of your performance guarantee schedule
- 4.4.6 What services are available to the District's staff on your website?
- 4.4.7 What reports are available to the District's staff online?
- 4.4.8 Do you capture/store, in your claims system, the following data:

Data Element	Yes/No	Data Element	Yes/No
Group/policy number		UB-92 bill type	
Employee ID number or other unique identifier		UB-92 revenue code	
Claimant ID number or other unique identifier		ICD codes	
Claimant relationship: employee, retiree, spouse and child		DRG code	
Claimant gender		CPT and/or CDT Code	
Claimant date of birth		CPT modifier	
Separate claims data for COBRA participants		Place of Service	
Provider name		Charged/billed amount	
Provider type code		Allowed amount	
Provider ID number (TIN and NPI)		Ineligible amount	
Provider address, city, state and zip code		Ineligible reason	
Provider network affiliation		Deductible, coinsurance and copayment amount	
Dates of service:		Paid Amount	
Date claim received		Timely pre-certification	
Claim processed/paid date			

Section Four: RESPONDENT QUESTIONNAIRE

Rev 022718

- 4.4.9 Do you have an active Voluntary Data Sharing Agreement (VDSA) or Voluntary Data Exchange Agreement (VDEA) with CMS where you share data on group health plan eligibility of individuals who are also eligible for Medicare coverage?
- 4.4.10 Will you be able to utilize the VDSA or VDEA to transfer data for the District in compliance with the Medicare Secondary Payer (MSP) Mandatory Insurer Reporting requirements?
- 4.4.11 Will you perform Coordination of Benefits (COB) as instructed in the District's plan document?
- 4.4.12 What procedures do you perform to determine the presence of other coverage (e.g., use claim detail, open enrollment query, annual query, etc.)?
- 4.4.13 The District may use a third party to conduct annual data mining. Confirm that the District will be able to get a tape of annual claims activity (including discount information) without any additional cost.
- 4.4.14 Has your organization had a recent Statement on Auditing Standards (SAS) 70 audit? If yes, when was the last one completed?

4.5 COBRA ADMINISTRATION

- 4.5.1 Do you provide COBRA administration services?
- 4.5.2 Do you provide the service in-house or are you subcontracting COBRA administration services? If you are subcontracting, please identify the vendor(s) you are proposing to use?
- 4.5.3 Please identify any costs that the District would need to pay for the administration, tools, services, etc. available for administration of the COBRA plan.
- 4.5.4 How long have you provided COBRA administration services?
- 4.5.5 Are you able to handle an auto reimbursement process?
- 4.5.6 Can your software accommodate a balance carry-over/grace period?
- 4.5.7 Can your organization send participants quarterly statements that include their balance?
- 4.5.8 Do you offer participants web access to view remaining claims balances and claims payment details (Itemized by date, amount, provider/service)?
- 4.5.9 Do you offer participants direct deposit of submitted claims into bank accounts?

4.6 FLEXIBLE SPENDING ACCOUNT ADMINISTRATION

- 4.6.1 Do you provide medial and dependent care FSA administration services?
- 4.6.2 Do you provide the service in-house or are you subcontracting FSA administration services? If you are subcontracting, please identify the vendor(s) you are proposing to use?
- 4.6.3 Please identify any costs that the District would need to pay for the administration, tools, services, etc. available for administration of the FSA plan.
- 4.6.4 Do you offer a card for use with the FSA?
- 4.6.5 How long have you provided FSA administration services?

Section Four: RESPONDENT QUESTIONNAIRE

Rev 022718

- 4.6.6 Which of the discrimination tests do you provide in the basic fee?
- 4.6.7 Are you able to handle an auto reimbursement process?
- 4.6.8 Can your software accommodate a balance carry-over/grace period?
- 4.6.9 Can your organization send participants quarterly statements that include their balance?
- 4.6.10 Do you offer participants web access to view remaining claims balances and claims payment details (Itemized by date, amount, provider/service)?
- 4.6.11 Do you offer participants direct deposit of submitted claims into bank accounts?
- 4.6.12 Ability to manage ACH and other electronic forms of payment

	Current Vendor FSA	Current Vendor COBRA	Proposed Vendor FSA	Proposed Vendor COBRA
Administration Fee (PEPM)				
Debit Card Fee (PEPM)				
Implementation/Setup Fee				
Custom Report Fees				
Rate Guarantee (# of Years)				
Total Monthly Cost (PEPM)				
Total Annual Cost (PEPY)				

4.7 TECHNICAL QUESTIONNAIRE

4.7.1 Underwriting Agreement

- 4.7.1.1 Will you provide claims lag reports at least annually, updating the monthly incurred and monthly paid claims? If no, why not?
- 4.7.1.2 Will your organization handle the District’s claims run out when the contract is terminated. If yes, for how long and how much will you charge for the administration of the claims run-out?
- 4.7.1.3 How do employees access services if they do not have an ID card?

4.8 SECURITY AND PRIVACY

4.8.1 Vendor must demonstrate its ability to comply with each requirement of this RFP. Its proposal must describe its security safeguards for both the transition and operating phases of the contract, including the encryption process and standards for Confidential Information. In addition to describing compliance with those contract terms, answer the following:

- 4.8.1.1 Describe how Confidential Information is stored. For information stored electronically, please advise whether the confidential information of other clients will be stored with that of MCCCCD.

Section Four: RESPONDENT QUESTIONNAIRE

Rev 022718

- 4.8.1.2 Describe the organizational structure and where the employees who will be working with MCCC'D's Confidential Data are located within that structure. Are employees background checked?
- 4.8.1.3 Describe whether you have had any incidences in the past five years in which you advised clients and their customers or employees of clients that their data may have been inappropriately accessed, exposed, or further disclosed without permission. Be specific in terms of number of incidences and numbers of customers or employees.

4.9 NETWORK QUESTIONNAIRE

- 4.9.1 Do you have a subnetwork of physicians which you deem high quality and highly efficient? If so, can you provide the scoring methodology how you rate these physicians? Is the scoring methodology for the provider's entire outcomes or is it per episode?
- 4.9.2 If you have the ability to steer members towards higher quality and efficient providers? If so, what percentage of the physicians qualify?
- 4.9.3 Do you have benefit differentials which allow member steerage towards higher quality physicians? Is this steerage benefit differential for all care by the provider or is it by episode of care?
- 4.9.4 Do you have benefit differentials which allow member steerage towards higher quality facilities? If so, is this steerage benefit differential for all care by the provider or is it by episode of care?

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:

5.1 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

5.2 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.

All proposals meeting the mandatory criteria will be evaluated by an evaluation committee. Award will be made to the offeror providing the most advantageous proposal under the RFP's terms.

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 3476-6, is authorized to submit this proposal on behalf of the company, and hereby offers to perform the services for the pricing indicated below:

6.1 PLAN FUNDING/DESIGN OPTIONS:

Match the current PPO plan designs on a self-funded basis. If you are a TPA proposing your services, you must include in your proposal the following services: medical network, pre-certification, utilization review, case management, disease management, centers of excellence, open enrollment services, ID cards, claim forms, claim reporting, claims payment, customer service, certificates and all appeals. Any deviations from the current plan design as requested must be separately noted. Qualifying proposals require 1st and 2nd year fixed rates with not to exceed rate increase guarantees for years 3 through 5 on all services.

PPO - Self-Funded	Monthly Rate 2022	Maximum % Increase 2023	Maximum % Increase 2024
List all fees on a Per Employee Per Month (PEPM) basis, unless requested otherwise.			
6.1.1 Pricing Fee: Indicate all fees MCCCCD will be subject to. Fees should assume that prescription drugs would be carved-out to an independent PBM. (NOTE: a PBM and stop-loss interface fee will not be accepted)			
Core Services			
Medical Plan Administrator			
Case Management			
Utilization Management			
Claims Fiduciary			
Data File Feed			
Telemedicine			
Network Access Fee			
Employee Assistance Program (EAP)			
Flexible Spending Account (FSA) Administration			
COBRA Administration			
Total Annual Estimated Fees			

6.2 Flexible Spending / COBRA Products & Services as requested in this RFP:

<u>Services</u>	<u>Price</u>

6.2.1 Prompt Payment Discount: _____

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 MCCCCD's purchase order terms ("Contract Documents") along with any engagement letter will constitute the provisions of the contract between MCCCCD and successful Proposer ("Contract"). MCCCCD 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 MCCCCD'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.

7.1 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:VIII or better. At the signing of this Agreement, Contractor shall furnish the MCCCCD 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, shall be endorsed to name MCCCCD and its agents, officers, officials, employees, and volunteers as additional insureds with the following language 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 MCCCCD 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 MCCCCD will not contribute to it. If any part of the Agreement is subcontracted, these insurance requirements also apply to all subcontractors.

Any modification or variation of the insurance requirements in this Contract shall be made by the MCCC Risk Management Department, whose decision shall be final. Such action 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 MCCC 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 MCCC shall not contribute to it. If any part of the Contract is subcontracted, these insurance requirements also apply to all subcontractors.

7.1.1 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

7.1.2 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.

7.1.3 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.

7.1.4 Network Security and Privacy Liability coverage in an amount not less than \$10,000,000 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 \$10,000,000 and payable whether incurred by MCCC 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 MCCC or on behalf of MCCC 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. MCCCCD shall be given at least 30 days' notice of the cancellation or expiration of the aforementioned insurance for any reason.

7.1.5 Professional Liability (Errors and Omissions Liability)

- Each Claim \$5,000,000
- Annual Aggregate \$5,000,000

a. In the event that the 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, either continuous coverage will be maintained, or an extended discovery period will be exercised, for a period of two (2) years beginning at the time work under this Contract is completed.

7.1.6 b. The policy shall cover professional misconduct or negligent acts for those positions defined in the Scope of Work of this contract.

7.2 OBLIGATIONS TO PROTECT CONFIDENTIAL INFORMATION

MCCCCD 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 MCCCCD 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. 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 MCCCCD employees and students, personal health information (as defined by the Health Insurance Portability and Accountability Act of 1996), and other personally identifiable information identified by applicable law or regulation. In addition, Confidential Information includes data and other information that is proprietary to or developed by MCCCCD such as institutional financial and performance records.

7.2.1 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.

7.2.2 If the Contractor potentially has access to MCCCCD 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. 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 to enhance or optimize the functionality of the service provided under the contract.

- 7.2.3 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 MCCCDC Confidential Information on a need-to-know basis to its subcontractors who are performing services, provided those subcontractors have executed confidentiality agreements and have agreed to materially the same or greater security obligations as Contractor provides with respect to MCCCDC Confidential Information hereunder, and further provided that Contractor shall remain legally and financially liable for any unauthorized disclosure of the MCCCDC Confidential Information by those subcontractors.

If a Contractor staff person or Contractor subcontractor potentially will have access to MCCCDC's network, facilities, data, Confidential Information, and/or Sensitive Information,¹ they may not perform any work involving such access until they have received MCCCDC's privacy and security training, and/or accepted and agreed to adhere to MCCCDC's privacy and security policies and procedures.² If exigent circumstances are presented, all or part of this requirement may be waived in writing by MCCCDC's Chief Privacy Officer or General Counsel.

- 7.2.4 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. MCCCDC designates Contractor and its employees and/or agents as an organization conducting certain studies for or on behalf of MCCCDC 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 MCCCDC and Contractor to release the information according to the authorization.
- 7.2.5 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.
- 7.2.5.1 These safeguards include, but are not limited to, implementation of adequate privacy

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.

² See, e.g., **MCCCDC Statement on Privacy** at <https://chancellor.maricopa.edu/public-stewardship/governance/administrative-regulations/4-auxiliary-services/4.22-statement-on-privacy>; **MCCCDC Written Information Security Program** at <https://chancellor.maricopa.edu/public-stewardship/governance/administrative-regulations/4-auxiliary-services/4.23-written-information-security-program>; and **MCCCDC 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>.

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 MCCCCD's information security and privacy policies and procedures as previously described herein. Contractor will supply the appropriate MCCCCD representative with copies of those policies and plans upon request.

- 7.2.5.2 Contractor will maintain personnel policies that appropriately check the backgrounds of its employees who will be providing services to MCCCCD. Contractor will supply the appropriate MCCCCD representative with copies of those policies upon request.
- 7.2.6 Contractor will inform MCCCCD'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 MCCCCD may be required to perform a risk assessment and/or provide a notification under applicable law, at which point MCCCCD 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 MCCCCD Office of General Counsel updated 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,
- 7.2.7 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. 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 MCCCCD, (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.

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 MCCCCD, 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 MCCCCD harmless from claims of any kind relating to the disclosure of MCCCCD 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.

- 7.2.8 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.
- 7.2.9 If applicable, during the term of the Contract, Contractor will be required to promptly update and resubmit the MCCCCD External Entity Due Diligence Questionnaire in Attachment to the RFP if it makes any revisions to its practices and policies that materially change its responses to that attachment.
- 7.2.10 If Contractor, its agents, employees, or any tier of Contractor's subcontractors in the performance of this Contract hosts or maintains MCCCCD 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.

7.3 RECORD AND DATA RETENTION, OWNERSHIP, ACCESS AND DECOMMISSIONING

- 7.3.1 As a political subdivision of the State of Arizona, MCCCCD 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, MCCCCD 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 MCCCCD 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.
- 7.3.2 MCCCCD owns all of the records and data of which Contractor has custody on MCCCCD'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 MCCCC representative. Contractor will work with MCCCC to transfer all of MCCCC's records and data to MCCCC on the termination or expiration of this Contract.
- 7.3.3 Contractor agrees to provide MCCCC access to records and Confidential Information that Contractor holds or uses on behalf of MCCCC upon written request of MCCCC with reasonable advance notice. Further, Contractor agrees to make amendments to Confidential Information as directed by MCCCC and will maintain a record of those changes.
- 7.3.4 Contractor agrees to maintain, and provide to MCCCC if requested, a record of when and to whom Confidential Information is disclosed.
- 7.3.5 MCCCC 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.
- 7.3.6 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.

7.4 MCCCC 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 MCCCC.

I. Definitions

The term "Authorized Visitor" means visitors who are pre-approved by MCCCC 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 MCCCC. 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 MCCCC'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 MCCCC 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 MCCCDC'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, MCCCDC 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 MCCCDC 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 MCCCCD'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 MCCCCD's network administrator (e.g., direct dial-up or DSL if permitted on MCCCCD's network). Unless otherwise specified in MCCCCD'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 MCCCCD's order, External Entity may also use a desktop/laptop client based product when it accesses the Environments residing on MCCCCD'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 MCCCCD'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 MCCCCD's network.

V. Data Management/Protection

Deletion of Environments: Upon termination of services or at MCCCCD'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. MCCCDC shall be entitled to request a recovery of such backed-up Environments within the six months following termination.

Reporting Security Incidents: If the MCCCDC 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 MCCCDC'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 MCCCDC's Environments has been misappropriated (including by an External Entity employee), External Entity will report such misappropriation to MCCCDC 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 MCCCDC's contract, MCCCDC's instructions, or to the extent required by law. External Entity will use diligent efforts to inform MCCCDC, 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 MCCCDC's request, External Entity will agree with MCCCDC on a schedule for periodic password changes.
- User IDs and passwords to MCCCDC's systems are not communicated to any other person without MCCCDC'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 MCCC'D'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 MCCC'D rules, when visiting MCCC'D 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 MCCC'D'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 MCCC'D'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 MCCCCD'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 MCCCCD'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.
- MCCCCD will be entitled to audit External Entity's Security Policies every year, once per year.

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 and other devices used to connect to the MCCCCD 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 MCCCCD External Entities may be asked to adopt; examples of sample verbiage are noted for some topics:

Section Seven: SPECIAL TERMS AND CONDITIONS

Rev 03/22/18

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 MCCCDC policy. Contractor will supply the appropriate MCCCDC representative with copies of those policies upon request.

Confidential Information

Sample Verbiage:

MCCCDC 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 MCCCDC 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 MCCCDC's network, facilities, data, and/or Confidential Information, they may not perform any work involving such access until they have received MCCCDC's privacy and security training, and/or accepted and agreed to adhere to MCCCDC'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 MCCCDC'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 MCCCDC 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:

³ See, e.g., **MCCCDC Statement on Privacy** at <https://chancellor.maricopa.edu/public-stewardship/governance/administrative-regulations/4-auxiliary-services/4.22-statement-on-privacy>; **MCCCDC Written Information Security Program** at <https://chancellor.maricopa.edu/public-stewardship/governance/administrative-regulations/4-auxiliary-services/4.23-written-information-security-program>; and **MCCCDC 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>.

Section Seven: SPECIAL TERMS AND CONDITIONS

Rev 03/2/18

- I. Meet or exceed MCCCC's information security and privacy policies and procedures as described herein,
- II. Do not conflict with MCCCC incident response requirements and, to the extent that they do, Contractor agrees to match and comply with MCCCC's requirements, and
- III. Retain the level of protection provided for MCCCC'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 MCCCC representative with copies of those policies and plans upon request.

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

Contractor shall inform MCCCC's Chief Privacy Officer and MCCCC'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 MCCCC may be required to perform a risk assessment and/or provide a notification under applicable law, at which point MCCCC 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 MCCCC 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 MCCCC 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 MCCCC, (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.

MCCCC 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 MCCCC 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 MCCCC, 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 MCCCC 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 MCCCC harmless from claims of any kind relating to the disclosure of MCCCC 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 MCCCC 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 the MCCCC External Entity Due Diligence Questionnaire, 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 MCCCC 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 MCCCC of a site hosted or maintained by Contractor or should this Agreement involve the access by Contractor to MCCCC'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 MCCCC 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

Section Seven: SPECIAL TERMS AND CONDITIONS

Rev 03/22/18

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 MCCCDC's Chief Privacy Officer and MCCCDC'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 MCCCDC may be required to perform a risk assessment and/or provide a notification under applicable law, at which point MCCCDC 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 MCCCDC 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 MCCCDC 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 MCCCDC, (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, MCCCDC 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, MCCCDC must retain records according to established retention periods. Records required for ongoing or foreseeable official proceedings such as audits, lawsuits or

Section Seven: SPECIAL TERMS AND CONDITIONS

Rev 03/2/18

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 MCCCDC records according to variable time periods/life cycles;
- b) Search and retrieve MCCCDC records based upon content;
- c) Place a litigation hold on MCCCDC records to ensure that they are not deleted;
- d) Grant direct access to MCCCDC for its own search and production of MCCCDC records;
- e) Preserve meta data;
- f) Produce MCCCDC electronic records; and
- g) Comply with the Americans with Disabilities Act.

MCCCDC owns all of the records and data of which Contractor has custody on MCCCDC'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 MCCCDC representative. Contractor shall work with MCCCDC to transfer all of MCCCDC's records and data to MCCCDC on the termination or expiration of the Contract.

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

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

MCCCDC 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.

MCCCDC 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>.

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 MCCC'D's purchase order terms ("Contract Documents") along with any engagement letter will constitute the provisions of the contract between MCCC'D and successful Proposer ("Contract"). MCCC'D 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 MCCC'D'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.

PARTIES TO AGREEMENT

The Contract shall be between the MCCC'D and the successful Proposer ("Contractor").

8.1 LIABILITY FOR TAXES

The Contractor is responsible for paying all taxes applicable to its operations, business property and income. MCCC'D shall not be liable for any tax imposed either directly or indirectly upon the Contractor, except that MCCC'D 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.

8.2 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.

8.3 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 MCCC'D authorized to sign contracts.

8.4 NO WAIVER

MCCC'D'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 MCCC'D'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.

8.5 FINANCIAL TRANSACTIONS

If the Contractor is responsible for handling any type of financial transaction for MCCCCD, 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 MCCCCD requests it in writing.

8.6 CONTRACT EXTENSION

Should the RFP provide options for extending the Contract beyond its initial term, MCCCCD 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 MCCCCD'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, MCCCCD 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 MCCCCD to do so.

8.7 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 MCCCCD 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.

8.8 INDEMNIFICATION

To the fullest extent permitted by law, Contractor shall defend, indemnify, and hold harmless MCCCCD, 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 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.

If applicable, Contractor shall also indemnify, defend and hold harmless MCCCCD and its officers, officials, employees and agents against any claim (including but not limited to attorney fees and court costs) that

their authorized use of Contractor's services or materials under this Agreement violates the claimant's property rights. Contractor shall be responsible for obtaining any intellectual property consents for materials or services that it provides under this Contract.

8.9 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.

8.10 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.

8.11 CONFLICT OF INTEREST

Notice is given of Arizona Revised Statutes §38-511 under which MCCCCD 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>

8.12 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.

8.13 AUDITS

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

8.14 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 MCCCCD. If the Contract specifies that MCCCCD will reimburse the Contractor a specific cost, Contractor may not charge MCCCCD that cost without MCCCCD approving a prior estimate of it. Additionally, MCCCCD reimburses travel and related expenses only at the rate that it reimburses its employees.

8.15 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

Section Eight: GENERAL TERMS AND CONDITIONS

Rev 032218

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. MCCCCD 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.

8.16 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 MCCCCD 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 MCCCCD 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.

8.17 CONTRACT TERMINATION

MCCCCD may terminate this Contract for convenience by giving Contractor 15 days' written notice of termination. MCCCCD 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. MCCCCD 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.

8.18 BREACH CURE; REPLACEMENT

The Contractor shall perform all requirements of the Contract in a manner consistent with the highest industry or professional standards. If MCCCCD 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 MCCCCD's sole discretion, the Contractor diligently pursues correction of the default and correction cannot be completed in 10 days, MCCCCD 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. MCCCCD is entitled to exercise all of its remedies under applicable law and in equity relating to Contractor's breach.

8.19 INTERPRETATION

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

8.20 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.

8.21 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.

8.22 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.

8.23 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.

8.24 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.

8.25 ADVERTISING AND PROMOTION

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

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

8.26 UNAVAILABILITY OF FUNDS

MCCCCD 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. MCCCCD shall give Contractor prompt written notice after it knows that funding will not be available.

8.27 NO WAIVER OF SOVEREIGN IMMUNITY

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

8.28 APPLICABLE LAW

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

8.29 PROPERTY RIGHTS

Except for pre-existing works of the Contractor or works of third parties for which Contractor has the permission to supply to MCCCCD under this Contract, MCCCCD 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 MCCCCD.

8.30 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 MCCCCD, the Contractor shall retain during performance and provide to MCCCCD 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. MCCCCD 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.

8.31 NOTICES

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

8.32 REVISIONS TO THE CONTRACT WORK OR PRICE

Contractor is on notice that the only MCCCDC representatives who may authorize revisions to the Contract are employees at MCCCDC'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 MCCCDC authorized to sign contracts. The person requesting a revision in the Contract, whether it is the Contractor or an MCCCDC employee, must provide the authorized MCCCDC 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, MCCCDC 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 MCCCDC'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. MCCCDC will determine whether the requested price increase or an alternate option is in its best interest.

8.33 GIFTS, GRATUITIES, UNRELATED COMPENSATION AND CONFLICTS OF INTEREST

In the interest of public stewardship, MCCCDC holds its employees, officers, and vendors to high ethical standards. Arizona state law prohibits an MCCCDC employee or officer from participating in any way in any MCCCDC decision, contract, sale or purchase if he or she has received something of value from an outside party whose interests are involved in that MCCCDC decision, contract, sale or purchase. Additionally, Arizona state law precludes any MCCCDC employee or officer from obtaining compensation of any kind for performing his or her responsibilities other than the compensation provided by MCCCDC. MCCCDC 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 MCCCDC 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 MCCCDC, to an MCCCDC employee or officer responsible for MCCCDC decisions, contracts, sales or purchases that may benefit Contractor or its subcontractors, suppliers or distributors.

8.34 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 MCCCCD 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 MCCCCD account:

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

10	Contractor's 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

Proposer must fill out and sign the following Data Security and Data Confidentiality Addendums. These addendums will be incorporated as Special Terms and Conditions upon contract award.



MARICOPA
COMMUNITY COLLEGES

MARICOPA COUNTY COMMUNITY COLLEGE DISTRICT
2411 West 14th Street, Tempe, AZ 85281-6942

DATA SECURITY ADDENDUM

THIS DATA SECURITY ADDENDUM (“ADDENDUM”) AS BETWEEN MARICOPA COUNTY COMMUNITY COLLEGE DISTRICT AND [VENDOR/CONTRACTOR] (“CONTRACTOR”) (AS DEFINED IN THE AGREEMENT) AMENDS THE AGREEMENT BETWEEN THE PARTIES DATED [DATE] (THE “AGREEMENT”), UNDER WHICH THE CONTRACTOR IS PROVIDING [DESCRIPTION OF SERVICES/SOLUTION], AND BY DOING SO, ADD THE FOLLOWING TERMS AND CONDITIONS AS AN ADDENDUM. THE PARTIES AGREE THAT THIS ADDENDUM WILL BE ATTACHED TO, INCORPORATED BY REFERENCE AND MADE A BINDING PART OF THE AGREEMENT. IN THE EVENT OF ANY CONFLICT AMONG THE TERMS OF THIS ADDENDUM AND THE AGREEMENT, THIS ADDENDUM SHALL TAKE PRECEDENCE AND THEREFORE CONTROL AND GOVERN THE PARTIES’ OBLIGATION WITH REGARD TO THE MATTERS HEREIN ADDRESSED.

1. Information Security Program.

1.1 Contractor will provide (and will cause its agents to provide) to MCCCCD their respective security measures, safeguards, and procedures for review and verification by MCCCCD of compliance with the terms of this Addendum and will confirm to MCCCCD 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 MCCCCD believes in good faith that continuing performance under the Agreement poses a security risk to MCCCCD or its data, network, or systems, MCCCCD may

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 MCCCCD. All other finding must be remediated within ninety (90) days. At MCCCCD'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 MCCCCD, 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 MCCCCD. Contractor will supply the appropriate MCCCCD 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 MCCCCD 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 MCCCCD 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 MCCCCD's Chief Privacy Officer or designated representative all known or suspected Security Incidents involving MCCCCD'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 MCCCCD may request. Contractor is required to cooperate with MCCCCD 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 MCCCCD 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 MCCCCD, Contractor shall engage, at Contractor's sole expense, technical experts approved by MCCCCD to investigate and analyze the impact of the Security Incident and to provide the report of results and conclusions of such investigation to MCCCCD. MCCCCD 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 MCCCCD for all costs incurred by MCCCCD 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 MCCCCD 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 MCCCCD, 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 MCCCCD'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 MCCCCD'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 MCCCCD'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.

Section Eleven: ATTACHMENT B

Rev 090817

2.8 If Contractor, its agents, employees, or any tier of Contractor’s subcontractors in the performance of the Agreement hosts or maintains MCCCCD Confidential Information on its technology, (i) Contractor warrants and confirms that the hosting or maintenance of MCCCCD’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. MCCCCD 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 MCCCCD, its business, or the services related to this Addendum; or (d) applicable law provides MCCCCD with a direct audit right.

MCCCCD
MARICOPA COUNTY COMMUNITY COLLEGE
DISTRICT

CONTRACTOR
Name of Contractor

Signature:

Name
Title

Date:

Signature:

Name
Title

Date:

Address:

Email:



MARICOPA
COMMUNITY COLLEGES

MARICOPA COUNTY COMMUNITY COLLEGE DISTRICT
2411 West 14th Street, Tempe, AZ 85281-6942

DATA CONFIDENTIALITY ADDENDUM

THIS DATA CONFIDENTIALITY ADDENDUM (“ADDENDUM”) AS BETWEEN MARICOPA COUNTY COMMUNITY COLLEGE DISTRICT AND [VENDOR/CONTRACTOR] (“CONTRACTOR”) (AS DEFINED IN THE AGREEMENT) AMENDS THE AGREEMENT BETWEEN THE PARTIES DATED [DATE] (THE “AGREEMENT”), UNDER WHICH THE CONTRACTOR IS PROVIDING [DESCRIPTION OF SERVICES/SOLUTION], AND BY DOING SO, ADD THE FOLLOWING TERMS AND CONDITIONS AS AN ADDENDUM. THE PARTIES AGREE THAT THIS ADDENDUM WILL BE ATTACHED TO, INCORPORATED BY REFERENCE, AND MADE A BINDING PART OF THE AGREEMENT. IN THE EVENT OF ANY CONFLICT AMONG THE TERMS OF THIS ADDENDUM AND THE AGREEMENT, THIS ADDENDUM SHALL TAKE PRECEDENCE AND THEREFORE CONTROL AND GOVERN THE PARTIES’ OBLIGATION WITH REGARD TO THE MATTERS HEREIN ADDRESSED.

1.Obligations to Protect Confidential Information

1.1 “Confidential Information” will include any and all MCCCCD 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 MCCCCD 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 MCCCCD.

Confidential Information does not include (i) information the Contractor already knows, (ii) information that becomes generally available to the public except as a result of disclosure by the Contractor in violation of this Addendum, and (iii) information that becomes known to the Contractor 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 MCCCCD in advance of such action and cooperate with MCCCCD to limit the extent and scope of such transfer or disclosure.

1.2 If the Contractor potentially has access to MCCCCD Confidential Information under the Agreement, 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 MCCCCD. Such use will not include examining Confidential Information for targeted marketing either within the confines of the service or external to the service (e.g., keyword indexing). Contractor may use anonymized and aggregated 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 MCCCCD Confidential Information is retained by Contractor.

1.3 Contractor will limit access to Confidential Information to its employees, contractors, and/or agents with a need to know the Confidential Information to carry out the activities under the Agreement and will instruct those employees to keep the information confidential. It is understood, however, that Contractor may disclose MCCCC 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 in writing to materially the same or greater security obligations as Contractor provides with respect to MCCCC Confidential Information hereunder, and further provided that Contractor shall remain legally and financially liable for any unauthorized disclosure or misuse of MCCCC Confidential Information by those employees, agents, contractors, and subcontractors. 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 MCCCC'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.

1.4 If a Contractor employee, contractor, or subcontractor potentially will have access to MCCCC's network, facilities, data, Confidential Information, and/or Sensitive Information⁴, they may not perform any work involving such access until they have received MCCCC's privacy and security training, and/or accepted and agreed to adhere to MCCCC's privacy and security policies and procedures⁵ and have entered into a non-disclosure agreement with MCCCC. If exigent circumstances are presented, all or part of this requirement may be waived in writing by MCCCC's Chief Privacy Officer or General Counsel.

1.5 Contractor understands that it may have access to student educational records, under the Agreement. MCCCC will designate Contractor and its employees and/or agents as school official for purposes of the Family Educational Rights and Privacy Act of 1974. Contractor will 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 Services. 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 MCCCC and Contractor to release the information according to the authorization.

1.6 Contractor may not use, disclose, sell, assign, loan, lease, dispose of, encumber or commercially exploit (or authorize any third party to do so) any Confidential Information for any purpose other than the strict performance of its duties and obligations under the Agreement. Contractor, including any division, subsidiary or affiliate of Contractor, will not be permitted to have access to, or use of Confidential Information except as required by law, other than as strictly required for its performance under the Agreement.

1.7 If the Contractor is responsible for handling any type of financial transaction for MCCCC, the Contractor shall demonstrate annually, as applicable, that it complies with the Statement on Standards for Attestation Engagements (SSAE) No. 18, known as SSAE 18, established by the Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA). The Contractor shall provide its annual

⁴Sensitive 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.

⁵ See, e.g., **MCCCC Statement on Privacy** at <https://district.maricopa.edu/regulations/admin-regs/section-4/4-22>; **MCCCC Written Information Security Program** at <https://district.maricopa.edu/regulations/admin-regs/section-4/4-23>; and **MCCCC Information Security Incident Response Plan** at <https://district.maricopa.edu/regulations/admin-regs/section-4/4-24>.

Section Eleven: ATTACHMENT B

Rev 090817

report, as applicable, on a reporting form or forms adopted as part of SSAE No. 18 no later than 30 days after MCCCC requests it in writing.

1.8 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 the Agreement. 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 MCCCC and Contractor to release the information according to the authorization. At all times during the Agreement, 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 agents involved in the Services also comply.

1.9 At all times during the term of the Agreement, Contractor will implement and maintain an information security program, which must include appropriate administrative, technical, physical, organizational, and operational safeguards and other security measures to maintain the security, privacy, availability, and confidentiality of Confidential Information in use, in motion and at rest. These safeguards include, but are not limited to, implementation of policies, procedures, and controls 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 MCCCC’s information security and privacy policies and procedures as previously described herein. Contractor will supply the appropriate MCCCC representative with copies of those policies and plans upon request.

1.10 Contractor’s information security program must include appropriate measures to protect the Confidential Information against unauthorized or unlawful processing and against accidental loss, destruction, damage, theft, alteration, misuse or disclosure. At a minimum, these should include (i) the requirements required under applicable privacy and data security laws (including 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)), (ii) the requirements set forth herein, and (iii) be in accordance with industry best practices. Contractor will review its information security program at least annually, or if significant changes occur, to ensure its continuing compliance, suitability, adequacy and effectiveness.

MCCCC
MARICOPA COUNTY COMMUNITY COLLEGE
DISTRICT

CONTRACTOR
Name of Contractor

Signature: _____
Name
Title

Date: _____

Signature: _____
Name
Title

Date: _____

Address: _____

Email: _____