MARICOPA COUNTY COMMUNITY COLLEGE DISTRICT

REQUEST FOR PROPOSAL # 3364-6

Online Tutoring Service

Proposal Due Date
March 30, 2017 3:00 P.M. (local time)

MARICOPA COUNTY COMMUNITY COLLEGE DISTRICT

RFP # 3364-6

Online Tutoring Service

A. SCHEDULE OF EVENTS

ACTIVITY	DATE
Release RFP	March 2, 2017
Questions Due	March 14, 2017
Proposals Due	March 30, 2017
In-Person Presentation/Interview (Invited)	Week of April 24
Proposed Contract Award	May 23, 2017

B. TABLE OF CONTENTS

ACKNOWLEDGMENT OF RECEIPT

RFP #: 3364-6

Description: **ONLINE TUTORING SERVICE**

Please provide the requested information below as acknowledgment that you have received our Request for Proposal noted above. It is **required** that interested Bidders complete this acknowledgment and return via Fax to MCCCD Purchasing at **(480) 731-8190** or email to purchasing@domail.maricopa.edu or by US Mail.

All addenda/amendments will continue to be posted on our website at http://www.maricopa.edu/business/purchasing/.

Failure to sign and return the "Acknowledge of Receipt" will result in your company not being sent any addenda to this RFP.

Name of Firm: _____

Address: _____

_____

Tel #: _____ Fax #: _____

E-Mail: _____

Name: (Print) _____Title:_____

Signature: _____Date: _____

PLEASE NOTE: Failure to respond to this acknowledgement **will** result in you company being removed from our bidders mailing list for this commodity.

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

1. GENERAL

1.1 INTRODUCTION

The Maricopa County Community College District (MCCCD) intends to engage with a service provider that will provide real-time tutoring and instructional support by qualified, credentialed tutors to students across all ten Maricopa colleges. The service will include tutoring for a variety of subjects, most significantly mathematics and English.

1.2 MCCCD DISTRICT MAKE-UP

The Maricopa Community Colleges comprise ten colleges, two skill centers, a Corporate College and numerous education centers dedicated to educational excellence by meeting the needs of businesses and the citizens of Maricopa County. Each college is individually accredited, yet part of a larger system, the Maricopa County Community College District. The District is one of the largest higher education systems in the world. 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. The Maricopa Community Colleges employs nearly 4,500 full-time faculty and staff and more than 9,000 part-time faculty and staff. Many management and staff positions (including clerical, crafts, food services, security, child care, maintenance and operations, custodial, grounds) become available throughout the year. All positions with the exception of certified safety officers are advertised individually as they occur. Maricopa Community Colleges is an equal opportunity employer of protected veterans and individuals with disabilities.

1.3 HISTORY

Maricopa ranks as one of the nation's largest systems of its kind and as the largest single provider of higher education in Arizona. Maricopa 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 Maricopa system. Maricopa'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 in 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. The Maricopa Community Colleges is a political subdivision of the state, and the elected governing board has the power to levy taxes. Funding comes from property taxes, state aid appropriations, student tuition, and federal, state and private grants.

2. PROPOSAL INSTRUCTIONS

2.1 PURPOSE OF RFP

The purpose of this solicitation is to obtain proposals from qualified companies to provide online tutoring services to be used by students at all ten(10) Maricopa Community Colleges.

2.2 PROPOSAL QUESTIONS

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

Mr. Larry Woo, Buyer I
(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 **March 14, 2017**. We will not respond directly to the company asking the question. Questions we feel need to be responded to will be answered in the form of an addendum and sent to potential respondents and posted on our website on/about **March 21, 2017.***

2.3 PROPOSAL SUBMISSION

It shall be the responsibility of the Proposer to assure that Proposals are received as follows:
The Proposal packet must contain one (1) original, seven (7) copies of the proposal and one (1) copy in PDF Format on a USB flash drive. The original must be clearly marked "Original" and the Proposal submission must be delivered Sealed.

The Proposals must be addressed to and received at the Main Reception Desk of MCCCD, address 2411 West 14th Street, Tempe, AZ, 85281, **no later than 3:00 P.M. (local time), March 30, 2017**. Proposals received after this time and date shall not be considered and will be returned unopened. When delivering your bid/proposal please allow for sufficient time to check in through the Security Desk.

The following information must be clearly visible on the outer most Proposal Packaging:

Request for Proposal # 3364-6, ONLINE TUTORING SERVICE
Proposal Closing Date: March 30, 2017 Time: 3:00 p.m. (local time)

NOTE: If you are hand carrying or having a proposal package hand delivered, you or the delivery agent should allow sufficient time to arrive, park, and go through security prior to dropping off your proposal package. This applies to any other method of delivery (FedEx, UPS,USPS, etc.) as well. Late proposals will not be accepted or considered for award. **Regardless of the method of delivery, it is your responsibility to insure on-time delivery of the proposal package.**

In submitting your proposal, make sure that it complies with Part IV – Proposal Requirements, Paragraph 4.3 – Deviations from RFP – to the extent that that paragraph is applicable to the terms of your submission.

2.4 PROPOSAL EVALUATION

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. If it does so, no contract award shall exist for purposes of the awardee initiating contract performance or incurring contract costs until an authorized representative of the District signs the contract document. If the District determines that the RFP and the selected awardee's proposal will constitute the contract, no contract award shall exist until the selected awardee receives a Notice of Award" from an authorized representative of the District and, if applicable, the approval of the District's Governing Board. Additionally, a selected awardee may not initiate contract performance or incur contract costs until it receives a District-issued purchase order.

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. The District discourages the submission of such information and undertakes to provide no more than reasonable efforts to protect the proprietary nature of such information. The District, as a public entity, cannot and does not warrant that proprietary information will not be disclosed. 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. No proposal shall exceed fifty (50) typewritten pages in length plus any pricing schedule(s), exhibits, resumes, or attachments.

2.7 MODIFICATIONS TO PROPOSALS

No oral, telephone, telegraphic, facsimile or computer data transfer proposals or modifications will be considered.

2.8 WITHDRAWAL OF PROPOSALS

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 by the District.

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

2.11 AWARD WITHOUT DISCUSSION

The District 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 will be made prior to commencement of performance. Initial performance period will be from May 23, 2017, or date of award, whichever is later, through June 30, 2019. MCCCD may at its discretion and with the concurrence of the successful proposer, exercise up to 3 one-year option periods for a total contract period not to exceed five years.

2.13 MCCCD MODIFICATIONS TO PROPOSALS

Any interpretation, correction, or change of this RFP will be made by written Addendum. Interpretations, corrections, or changes of this RFP made in any other manner will not be binding, and Proposers shall not rely upon such interpretations, corrections, and changes. Any changes or corrections will be issued by MCCCD Purchasing. Addenda will be mailed or faxed to all that are known to have received a copy of the RFP. Addenda will also be posted to the proposal documents on the Purchasing website located at www.maricops.edu/purchasing. **Since failure to acknowledge any addendum(s) may be cause for rejection, Proposers must return the addendum-completed acknowledgment(s) prior to or with the proposal.**

2.14 NON-COLLUSION

The District 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 District'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 District from obtaining the lowest possible competitive price.

3. GENERAL TERMS AND CONDITIONS

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

3.1 PARTIES TO AGREEMENT

The Contract shall be between the Maricopa County Community College District and the successful Proposer ("Contractor").

3.2 LIABILITY FOR TAXES

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

3.3 FORCE MAJEURE

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

3.4 CONTRACT ASSIGNMENT

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

3.5 NO WAIVER

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

3.6 FINANCIAL TRANSACITONS

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

3.7 CONTRACT EXTENSION

Should the RFP provide options for extending the Contract beyond its initial term, MCCCD reserves the right to exercise those options without prior written notice and by the issuance of a purchase order to the Contractor. If

the Contractor does not wish to renew the Contract, it must submit a written notice of its desire to cancel, which must be received by MCCCD's Purchasing Department no later than ninety (90) days prior to the end of the current term.

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

3.8 FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT

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

3.9 INSURANCE REQUIREMENTS

The Contractor shall maintain during the term of the Contract (including any renewals of the initial term) the insurance policies specified in this Paragraph issued by companies licensed in Arizona with a current A.M. Best rating of A:VIII or better. Before the start of Contract performance, MCCCD may direct the Contractor to furnish the MCCCD Risk Manager with certificates of insurance evidencing the required coverage, conditions, and limits required by the Contract at the following address:

MCCCD Risk Manager
2411 West 14th Street
Tempe, AZ 85281-6942
Tel: 480-731-8879 / Fax: 480-731-8890

The insurance policies, except Workers' Compensation and Professional Liability, must be endorsed to name MCCCD, its agents, officers, officials, employees, and volunteers as additional insured with this language or its equivalent:

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

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

3.9.1 **Commercial General Liability** insurance with a limit of not less than $1,000,000 per occurrence, $2,000,000 in the aggregate, for bodily injury, property damage, personal injury, and products and completed operations, including but not limited to, the liability assumed under the indemnification provisions of this Contract.

3.9.2 **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 owned, hired, and non-owned vehicles.

3.9.3 **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.

3.9.4 If applicable, **Professional Liability** insurance covering acts, errors, mistakes, and omissions arising out of the work or services performed by the Contractor, or any person employed by the Contractor, with a limit of not less than $1,000,000 each claim.

3.9.5 If applicable, **Network Security and Privacy Liability** coverage including costs of investigating and responding to a potential or actual breach of confidential information (e.g., computer forensic investigation, public relations response, outside counsel, notification mailing, call center, voluntary notification, credit monitoring and identity restoration costs, costs incurred in connection with any regulatory investigation, fines (including PCI fines), penalties assessed by regulator, and defense costs with limit of not less than $2 million per claim/$2 million aggregate.

3.10 INDEMNIFICATION

To the fullest extent permitted by law, Contractor shall defend, indemnify, and hold harmless MCCCD, its agents, officers, officials, employees, and volunteers from and against all claims, damages, losses, and expenses (including but not limited to attorney fees and court costs) arising from 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 MCCCD 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.

3.11 OBLIGATIONS TO PROTECT CONFIDENTIAL INFORMATION

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

For purposes of this Contract, Confidential Information is defined as any and all MCCCD information and data whose collection, sharing, dissemination, use, preservation, disclosure, protection, storage, destruction and/or disposition is governed by federal, state, local and/or international law or regulation. Confidential Information includes, but is not limited to, Social Security Numbers, student records, student financial records regarding students (or their parents or sponsors), financial and personal information regarding MCCCD employees and students, 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 MCCCD such as institutional financial and performance records.

3.11.1 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.

3.11.2 If the Contractor potentially has access to MCCCD Confidential Information under this Contract, Contractor agrees that Confidential Information provided to it, or to which it may have access, during the provision of service, will be used only and exclusively to support the service and service execution and not for any other purpose. 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.

3.11.3 Contractor will limit access to Confidential Information to its employees with a need to know the Confidential Information to carry out the activities under this Contract and will instruct those employees to keep the information confidential. It is understood, however, that Contractor may disclose the MCCCD Confidential Information on a need-to-know basis to its 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 MCCCD Confidential Information hereunder, and further provided that Contractor shall remain legally and financially liable for any unauthorized disclosure of the MCCCD Confidential Information by those subcontractors.

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

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

3.11.5 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.

3.11.5.1 These safeguards include, but are not limited to, implementation of adequate privacy and security policies and data breach response plans that comply with industry standards and the requirements of applicable laws and the regulatory agencies responsible for enforcing them, as long as they meet or exceed MCCCD's information security and privacy policies and procedures as previously described

---

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

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

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

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

3.11.7 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.

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

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

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

3.11.11 If applicable, during the term of the Contract, Contractor will be required to promptly update and resubmit the **MCCCD External Entity Due Diligence Questionnaire** in Attachment C to the RFP if it makes any revisions to its practices and policies that materially change its responses to that attachment.

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

3.12 RECORD AND DATA RETENTION, OWNERSHIP, ACCESS AND DECOMMISSIONING

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

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

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

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

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

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

3.12.6 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.

3.13 PERMITS

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

3.14 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.

3.15 CONFLICT OF INTEREST

Notice is given of Arizona Revised Statutes §38-511 under which MCCCD may cancel a contract without recourse for any conflict of interest described in that law.
See: http://www.azleg.gov/FormatDocument.asp?inDoc=/ars/38/00511.htm&Title=38&DocType=ARS

3.16 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.

3.17 AUDITS

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

3.18 UNAUTHORIZED COSTS OR COSTS OUTSIDE SCOPE OF AGREEMENT; TRAVEL

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

3.19 NON-DISCRIMINATION

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

3.20 COMPLIANCE WITH IMMIGRATION LAWS; LEGAL WORKER'S ACT

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

applicable laws that apply to it and this Contract, including executive orders of the Governor of the State of Arizona.

3.21 CONTRACT TERMINATION

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

3.22 BREACH CURE; REPLACEMENT

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

3.23 INTERPRETATION

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

3.24 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..

3.25 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.

3.26 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.

Cooperative purchasing on this contract is not considered permissible until MCCCD and Contractor execute a separate Cooperative Purchasing Agreement that shall be attached to the contract as an amendment.

3.27 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, 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 FROM THE MCCCD PURCHASING DEPARTMENT.

3.28 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.

3.29 ADVERTISING AND PROMOTION

The name or logos of the MCCCD or those of any of the colleges, skill centers, or programs under MCCCD's jurisdiction shall not be used by Contractor except as may be required to perform this Contract and only as approved under MCCCD's "Use of MCCCD Marks" regulation at:
http://www.maricopa.edu/publicstewardship/governance/adminregs/auxiliary/4_19.php

3.30 UNAVAILABILITY OF FUNDS

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

3.31 NO WAIVER OF SOVEREIGN IMMUNITY

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

3.32 APPLICABLE LAW

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

3.33 PROPERTY RIGHTS

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

3.34 DOCUMENTATION OF ANALYSES TO SUPPORT FINDINGS, CONCLUSIONS AND RECOMMENDATIONS

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

3.35 NOTICES

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

3.36 REVISIONS TO THE CONTRACT WORK OR PRICE

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

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

3.37 GIFTS, GRATUITIES, UNRELATED COMPENSATION AND CONFLICTS OF INTEREST

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

3.38 DISABILITY STANDARDS.

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 Standards 2.0 at Level AA. Contractor agrees to promptly respond to and resolve any complaint regarding accessibility of its products or services. Contractor must provide, on request, accessibility testing results and written documentation verifying accessibility. Contractor further agrees to indemnify and hold harmless MCCCD from any claims arising out of its failure to comply with the aforesaid requirements. Failure to

comply with these requirements shall constitute a material breach and be grounds for termination of this Agreement.

4. PROPOSAL REQUIREMENTS

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

4.1 MINIMUM REQUIREMENTS

4.1.1 Must be licensed by the State the business is in, if services requested require such licensure.

4.1.2 Must provide a completed pricing schedule (Section 8) signed by an authorized company signatory.

4.1.3 Must have carefully read and understand all parts of the RFP and certified that the Proposal is made in accordance therewith.

4.1.4 Must submit written answers to the respondent questionnaire (Section 7). All answers must be in the order in which the questions were asked.

4.2 SPECIFIC REQUIREMENTS

4.2.1. Functional Requirements

4.2.1.1 Tutoring will be available in the following subjects at a minimum:

4.2.1.1.1 Mathematics
4.2.1.1.2 English (writing)
4.2.1.1.3 Spanish
4.2.1.1.4 Physics
4.2.1.1.5 Biology
4.2.1.1.6 Chemistry
4.2.1.1.7 Nursing
4.2.1.1.8 Accounting
4.2.1.1.9 Economics
4.2.1.1.10 Business

4.2.1.2 Services are provided by tutors that have a Bachelor's degree (not necessarily in the subject they will be tutoring) or equivalent for occupational areas (e.g. RN for Nursing tutors).

4.2.1.3 Core tutoring services will be provided twenty-four (24) hours per day, seven days per week.

4.2.1.4 Customer support will be available twenty-four (24) hours per day, seven days per week.

4.2.1.5 Training will be provided for use and administration of service, for both staff and students.

4.2.2. Technical Requirements:

4.2.2.1 The service must provide integration for students to access tutoring from within the Canvas Learning Management System (LMS).

4.2.2.2 The service must provide ability for students to access tutoring from within an internally-developed SharePoint-based LMS.

4.2.2.3 The service must provide ability for students to access tutoring directly through the web without navigating through an LMS.

4.2.2.4 The service should provide capacity for audio-enabled and/or video-enabled tutoring sessions.

4.2.2.5 The service must provide ability to review individual students and their tutoring sessions using recorded sessions or other methods of session capture.

4.2.2.6 The service must provide reporting and analytics by college and aggregated for all colleges, as well as by student, subject, and number of hours used.

4.2.2.7 System must be accessible using industry standard web browsers.

4.2.2.8 The system must provide data privacy in compliance with the Family Educational Rights and Privacy Act (FERPA).

4.2.2.9 Completion of the attached MCCCD External Entity Due Diligence Questionnaire (Attachment C) will be requested upon determination of a susceptibility of award.

4.3 DEVIATIONS FROM RFP

Proposers must specifically provide a separate listing of each circumstance in which their proposal differs from any terms or conditions of the Request for Proposals. 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 the RFP shall result in rejection of the proposal.

The term "material deviations" includes both deviations from the District contract terms set forth in this RFP **and** additional contract terms that the Proposer requests the District 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 District considers the General Terms and Conditions of this RFP to be a fair allocation of risk between a contractor and the District. It will not accept terms – revised or additional ones - that shift those risks or provide the Proposer with additional discretion. The Proposer in choosing the respond to this RFP, must demonstrate in its Proposal that it accepts the terms upon which the District is conducting the competition.

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

4.4 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.

4.5 AWARD CONSIDERATION

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

4.6 IN-PERSON PRESENTATION

Should any proposal be deemed susceptible for award MCCCD may require an in-person presentation/interview which will include a demonstration of the proposer's solution as well as to answer any additional questions needed to make a decision to award. The week of April 24, 2017 has been tentatively targeted to hold these interviews. MCCCD will notify proposers as soon as possible that they have been selected and when the interview date will be set so travel arrangements may be made.

5. SCOPE OF WORK

5.1 ENVIRONMENT:

MCCCD is a single district with ten separately accredited colleges and a district office. Students generally self-identify with a single institution, however approximately 10% of students attend more than one MCCCD college in the same term, and over 50% have attended more than one Maricopa college in their lifetime. Maricopa is actively pursuing several initiatives to standardize, centralize, or otherwise provide consistent service to students as they pursue their academic career across the Maricopa colleges. The implementation of a consistent approach to online tutoring for the Maricopa County Community College District is one planned outcome of these initiatives.

At the district level, all Maricopa students have an enterprise-wide Maricopa Enterprise ID (MEID) account and password used to authenticate and gain access to technology systems access. Students have student email powered by Google Apps for Education, an online student center for enrollment and student records activities powered by PeopleSoft Campus Solutions, and nine of the colleges provide access to the Canvas learning management system. Rio Salado is the only college using an LMS other than Canvas. Their homegrown solution, called RioLearn, is described below.

RioLearn is a proprietary learning management system developed and used by Rio Salado College, a primarily-online college with an enrollment of approximately 25,000 in Fall of 2012. RioLearn is hosted on-site and is built on a framework of Microsoft SharePoint with custom .NET programming.

From July, 1 2015-June 30, 2016, MCCCD utilized a combined total of over 7,000 hours of online tutoring services.

The goal of this RFP is to implement a standard system/service for online tutoring access across MCCCD.

5.2 SCOPE OF WORK:

If services are to be accomplished through an affiliation with another company or consultant, the information requested below should be completed for each company. Explicitly identify the lead company. Each company will be evaluated based on the criteria requested in the RFP.

5.2.1 Functional

5.2.1.1 List tutoring subjects, available levels, and identify which require advanced scheduling (as opposed to real-time on-demand engagement). Ensure that all subjects identified in 4.2.1.1 are addressed.

5.2.1.2 Describe hiring qualifications for tutors, including required credentials/experience and how qualifications are verified.

5.2.1.3 Describe professional development and/or ongoing training, both required and optional, for tutors.

5.2.1.4 Detail service availability hours, and any services (e.g. beyond core services) not available 24 hours per day, seven days per week.

5.2.1.4.1 Detail services available specifically during Winter Intersession, between 12/15 and 1/20, and any gaps in service during that time.

5.2.1.5 Describe training available, both for end users (students) and staff/administrators.

5.2.1.6 Describe any ancillary resources available to students other than tutoring sessions, and any costs associated with them.

5.2.1.7 Describe options for purchasing additional blocks of tutoring hours, possible usage tiers and discounted rates as well as options to roll unused, pre-paid, hours into the subsequent contact year.

5.2.1.8 Describe any ability to access the system for demonstration purposes, instructor access, etc.

5.2.1.9 Describe / identify file formats available to students wanting to share / upload their work.

5.2.1.10 Describe steps, including screenshots if appropriate, for students to receive tutoring in a specific subject.

5.2.1.11 Describe ability for multimedia tutoring sessions, including screenshots if appropriate. Identify any required student software or browser extensions needed for multimedia sessions.

5.2.1.12 Describe steps, including screenshots if appropriate, for a tutor to record comments regarding a tutoring session.

5.2.1.13 Describe steps, including screenshots if appropriate, for a college tutoring director with appropriate access to review a specific student's tutoring session. Identify what session information would be available.

5.2.1.14 List default reports that are available to administrative users.

5.2.1.15 Describe formats available for data extracts, reporting, etc.

5.2.1.16 Describe steps, including screenshots if appropriate, for developing a custom report.

5.2.1.17 Describe any integrations available for student success early alert systems.

5.2.1.18 Detail ability to limit access by number of hours, by student, by subject, by college, and other administrative options / functions.

5.2.1.19 Describe how your system meets the federal requirements of the Family Educational Rights and Privacy Act (FERPA).

5.2.1.20 Describe the system's alignment with accessibility guidelines, WCAG 2.0, and the level (A, AA, AAA) of compliance provided. Include a description of what this generally means for a student with a disability.

5.2.1.21 Describe the functionality available when the product is integrated into the Canvas Learning Management System.

5.2.1.22 Describe any differences in functionality when integrated into an internally-developed SharePoint-based Learning Management System.

5.2.1.23 Describe any differences in functionality when access is via a simple web page.

5.2.1.24 Describe / identify the supported web browsers as well as any plugins and/or extensions that are needed.

5.2.2 Technical

5.2.2.1 Describe ability to integrate with MCCCD-operated authentication systems, using mechanisms such as LDAPS, CAS, ASFS, etc.

5.2.2.2 Describe the expected personnel resource (hours) and skills required to maintain any technical aspect of the system (such as authentication) after it is implemented.

5.2.2.3 Describe the service options available, and the recommended service level agreement, regarding system availability. Include any customer reimbursement strategy for failure to deliver to the agreement.

5.2.2.4 Describe the service options available, and the recommended service level agreement, regarding system capacity (response times) when interacting with the system and when interacting during a tutoring session. Include any customer reimbursement strategy for failure to deliver to the agreement.

5.2.2.5 Describe the escalation process Maricopa would use in the case of a tutoring system outage or connectivity failure.

5.2.2.6 Describe any automated alerts and/or, notifications of system outages or in-availability to render services that will be provided to Maricopa.

5.2.2.7 Describe any availability and capacity reporting that would be provided to Maricopa following a major incident – such as a two hour system outage or unavailability.

5.2.2.8 Describe any availability and capacity reporting that would be provided to Maricopa on a regular interval -such as monthly or quarterly.

5.2.2.9 Describe / identify client operating systems supported (including mobile) and any required client software. Address the matter of responsive design provided for smaller screen real-estate.

5.2.2.10 Describe the technique(s) used for a Canvas LMS integration.

5.2.2.11 Describe the technique(s) used for a SharePoint-based LMS integration.

5.2.2.12 Describe the technique(s) used for a simple web page integration.

5.2.2.13 Describe / identify all student specific data that would be maintained within the system.

5.2.3 Organizational

5.2.3.1 Has this platform been used at similar size organizations? Has it been used at similarly structured institutions of higher education?

5.2.3.2 Why should MCCCD choose your product and your company? Please provide a concise narrative as to why your product and your company are best able to serve MCCCD. Include any key items about your company and unique features of your product that distinguishes it above others.

5.2.3.3 What support options are available? Please describe the levels and the recommended support options for MCCCD.

5.2.3.4 Furnish any case studies that help us understand your business model for tutoring services including other solutions your company currently provides.

5.3 MCCCD / PROVIDER RELATIONSHIP:

5.3.1 Describe the typical relationship and personnel involved between your organization and an institution such as MCCCD. Who are the key contacts at your company and their roles? (e.g. Account Representative, Technical Support Representative, etc.)

5.3.2 What is the hierarchy or organizational structure of the personnel MCCCD would interact with?

5.3.3 Describe how the MCCCD relationship would be handled as a large client compared to a client of a smaller size.

5.3.4 What kinds of events and user communities are available and/or supported by the provider in order to learn from other users and clients?

5.3.5 Provide detailed description of training required for content managers to use the tool. Describe training methodologies offered, including options for on-site training, web-based training, participation at regional training seminars, refresher training, compliance training, etc.

5.3.6 Describe the options and levels of support, warranty coverage, and types of maintenance agreements that are available for the proposed system.

5.4 ADDITIONAL SERVICES

Proposer may offer, on a separate page referencing this Section 5.4, additional goods and/or services including associated costs/prices that are not addressed in Section 8. The District retains the absolute and sole discretion to examine and consider these additional goods/service options for inclusion in the contract awarded under this RFP.

6. EVALUATION CRITERIA

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

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

6.2 Specific areas that will be evaluated and scored except as described in STEP THREE below:
- A. Past experience in providing comparable services to other clients.
- B. Responses to Minimum and Specific Requirements.
- C. Respondent Questionnaire responses.
- D. Pricing.

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. The lowest dollar priced service **may** or **may not** indicate the successful proposer. Price constitutes only one of several evaluation criteria. 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.

7. RESPONDENT QUESTIONNAIRE

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

7.1 Company Overview

7.2 Corporate Structure
- 7.2.1 Legal entity
- 7.2.2 State of registration or incorporation
- 7.2.3 Public company – listing symbol
- 7.2.4 Majority ownership

7.3 Operating history
- 7.3.1 Years in business
- 7.3.2 Growth rate
- 7.3.3 Services
- 7.3.4 Hours of operation
- 7.3.5 Financial condition

7.4 Core Business Strategy

7.5 Technology roadmap

7.6 Organization structure

7.7 Technology and networks overview

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

8. Pricing Schedule

The undersigned has read and understands all conditions and terms of RFP 3364-6, is authorized to submit this proposal on behalf of the company, and hereby offers to perform the services for the **pricing** indicated below:

8.1 Products/Services as requested in this RFP (hourly rate, total, or other pricing method). Itemize any initial/one-time costs as well as options for additional tiered discount structures if historical usage is exceeded:

Base Hourly Rate: $_____ HR

One-time set-up costs (provide detail):

_____$_____
_____$_____
_____$_____

Discount Tiers (list number of hours necessary before new pricing takes effect):

_____$_____ HR
_____$_____ HR
_____$_____ HR
_____$_____ HR

8.2 Prompt Payment Discount:

8.3 Other discounts available:

Other required services/fees, if any, not specifically requested in the RFP (list below):

_____$_____
_____$_____
_____$_____
_____$_____

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 next page must be completed, signed and included with your proposal.

9. 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 **five (5) 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? _____

ATTACHMENT A

ADDITIONAL BUSINESS INFORMATION (continued)

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

_____

_____

_____

9. Account Manager Information:

Name: _____

Phone: _____

Pager: _____

10. Contractors License Number(s):

TYPE	NUMBER
_____	_____
_____	_____

11. Do you ever sub-contract any of your services?

_____ NO

_____ YES

If YES, which services?: _____

_____

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

ATTACHMENT B

MCCCD STUDENT INFORMATION SYSTEM
NON-DISCLOSURE AGREEMENT

_____
Name

_____
Date

_____
Job Title

_____
Company Name

I, _____, agree that when given access to the Maricopa County Community College District Student Information System (SIS) database or file,

I will not reveal or attempt to reveal any individually identifiable information furnished, acquired, retrieved, or assembled by me in connection with the SIS database for any purpose;

I will not disclose to the public or otherwise, information from which a student's records could be identified;

I will not permit any other person to use a SIS account or password;

I will not attempt to identify individual students in the SIS database by joining that data with other data available to me;

I will ensure that information extracted from the SIS database is safeguarded and stored in a location and medium not accessible to anyone else but a MCCCD authorized person;

I will report any loss or breach of security to the MCCCD Purchasing Office (Attn: Keith Killourie / 480-731-8518) immediately;

I have read and agree to be bound by the Non-Disclosure Agreement between Maricopa County Community College District and my Company.

_____
Signature / Date

_____
Company Name

ATTACHMENT C

MCCCD EXTERNAL ENTITY DUE DILIGENCE QUESTIONNAIRE

A completed MCCCD External Entity Due Diligence Questionnaire is not required with an initial submission of your proposal. Should your proposal be deemed susceptible for an award this questionnaire will need to be completed and returned back to the MCCCD Purchasing Department within 7 days for a Security and Privacy review by both MCCCD's Legal and Information Technology Services (ITS) Departments.

Failure to completely fill out and return the form by the requested deadline date may be grounds to disqualify your proposal from award consideration.

Failure to answer subsequent questions or comply with any requests by the Legal and the ITS Departments may also disqualify your proposal from award consideration.

ATTACHMENT C

MCCCD EXTERNAL ENTITY DUE DILIGENCE QUESTIONNAIRE

FOR COMPLETION BY EXTERNAL ENTITY

SECURITY AND HOSTING STANDARDS AND PRACTICES

Instructions for Completion of this Questionnaire:
This questionnaire must be completed if the product or service that MCCCD is being asked to adopt involves data and information that is not exclusively stored at MCCCD. By completing this questionnaire, you are verifying that your responses are based on personal knowledge and that they are the result of your due diligence to provide accurate and comprehensive information about the matter at hand.

Name of External Entity: Click here to enter text.

First and Last Names of Preparer: Click here to enter text.

Date of Completion: Click here to enter a date.

By submitting this questionnaire, I certify that I have read and agree to its contents. I attest to the validity of the responses provided herein and I certify that all responses are (i) based on my personal knowledge and (ii) the result of my due diligence to provide accurate and comprehensive information about the matter at hand.

The following table lists various security and privacy-related reports for which we ask that you provide information. Please select the correct drop-down box entry for each of the following report types to indicate whether your organization has been the subject of an audit by an independent organization which evaluates and provides an opinion on the existence and effectiveness of information security controls.

Report Type 1: Department of Defense Certification and Accreditation	**Choose an item.**
Report Type 2: FISMA Audit	**Choose an item.**
Report Type 3: SSAE16	**Choose an item.**
Report Type 4: SOC 1, SOC 2 or SOC 3 **[Note: The SOC 3 report is generally available and does not require an NDA; however, if your organization can provide only the SOC 1 or SOC 2, MCCCD Legal is willing to sign an NDA prior to disclosure.]**	**Choose an item.**
Report Type 5: PCI DSS Audit	**Choose an item.**
Report Type 6: HIPAA Audit	**Choose an item.**
Report Type 7: Other Audit by an independent organization which evaluates and provides an opinion on the existence and effectiveness of your organization's information security controls (e.g., certification regarding a Learning Tool Interoperability (LTI) in Canvas).	**Choose an item.**

If you answered "Yes" to one or more of the above report types, please provide evidence or attach a copy of the corresponding report(s) with your response. You do not need to respond to the remaining questions.

If you answered "No" to each of the above report types, please complete the remainder of the questionnaire and submit it and all related documentation with your response.

For each of the following questions, please provide a copy of your organization's policy or other documentation that addresses the particular item. Please provide as much detail as possible in your responses. Feel free to include links to websites where further explanations may be found.

[EMBED POLICIES, MANUALS, REPORTS AND RELATED DOCUMENTATION IN THIS TABLE]

2.0 Security Policies

2.1 Organizational Security

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
1.	Are the following teams and individuals involved in information security at external entity and are their roles and responsibilities clearly defined? a) Executive-level oversight committee b) Corporate information c) All lines of business (LoBs) d) Individual information security managers who are assigned by each LoB		
2.	Do external entity's information security policies and practices include in sufficient detail guiding principles for: a) Development? b) Executive approval? c) Implementation? d) Maintenance?		
3.	Do external entity's information security policies promote the practice of: a) Compartmentalization of information? b) Least privilege? c) Need-to-know? d) Segregation of duties?		
4.	Are the following individuals subject to external entity organizational security policies?		

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
	a) All full-time and part-time employees? b) Temporary employees? c) Independent contractors[3] and subcontractors[4]?		
Additional Comments:			

2.2 Asset Classification and Control

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
1.	Does external entity policy define the following information assets as protected data and promote adherence to minimum handling requirements by all external entity personnel? a) Personally Identifiable Education Records - Covered under Family Educational Rights and Privacy Act (FERPA) b) Personally Identifiable Financial Information (PIFI/spiffy) - Covered under Gramm–Leach–Bliley Act (GLBA aka Financial Services Modernization Act of 1999) c) Payment Card Information (PCI/epic) - Covered under Payment Card Industry Data Security Standard (PCI DSS) d) Protected Health Information (PHI/phi) - Covered under the Health Insurance Portability and Accountability Act of 1996 (HIPAA)		
2.	Does external entity policy require implementation of anti-virus and personal firewall software?		
3.	Does external entity policy strongly recommend use of a computer program to manage the distribution of updates and hotfixes to computers in a corporate environment?		
4.	Do external entity asset classification and control security policies apply to the following		

[3] The term "independent contractor(s)" means independent contractors retained by external entity and its subsidiaries that provide services for the benefit of the external entity and its subsidiaries.
[4] The term "subcontractor(s)" means subcontractors retained by external entity and its subsidiaries that assist in performing all or any part of the services which the external entity has undertaken to perform.

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
	individuals? a) All full-time and part-time employees? b) Temporary employees? c) Independent external entities and subcontractors?		
5.	Do external entity policies establish requirements for acceptable non-personal business-related use of external entity's: a) Corporate network? b) Computer systems? c) Telephony systems? d) Messaging technologies? e) Internet access? f) Reprographic systems? g) Other company resources?		
Additional Comments:			

2.3 Human Resource Security

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
1.	Does external entity have a code of ethical conduct that: a) Establishes high standards for ethics and business conduct? b) Applies to every level of the company? c) Applies to every location where external entity does business throughout the world? d) Applies to all full-time and part-time employees? e) Applies to temporary employees? d) Applies to independent contractors and subcontractors? e) Covers the topic of legal and regulatory compliance? f) Covers the topic of business conduct and relationships?		

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
	g) Requires compliance-tracked training that occurs biennially (i.e., once every 2 years) in: a. Ethics? b. Business conduct? c. Sensitive information handling?		
Additional Comments:			

2.4 Physical and Environmental Security

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
1.	Does external entity policy establish corporate-level mandates for complying with the U.S.-European Union Safe Harbor Program's EU Data Protection Directive of 1998 on maintaining the privacy and integrity of personal data?		
2.	Does external entity policy establish mandates for frequently undergoing the second of three AICPA (American Institute of CPAs) Service Organization Controls audits (i.e., the "SOC 2" audit) to measure the following controls related to external entity's provision of IT and data center services: a) Security? b) Availability? c) Processing integrity (ensuring system accuracy, completion and authorization)? d) Confidentiality? e) Privacy?		
3.	Does external entity policy provide corporate-level mandates for log retention, review and analysis covering: a) Minimum log requirements? b) Responsibilities for the configuration and implementation of logging? c) Alert review? d) Problem management? e) Retention? f) Security and protection of logs?		

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
	g) Compliance review?		
4.	Does external entity policy establish information erasure guidelines that cover: a) Data erasure from all types of electronic media? b) Cost-benefit analysis of physical destruction vs. post-sanitization recycling?		
Additional Comments:			

2.5 Access Control

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
1.	Does external entity policy describe logical access control requirements for all external entity systems, including: a) Authentication? b) Authorization? c) Access approval? d) Provisioning? e) Revocation for employees and other external entity-defined 'users' with access to external entity systems that are neither internet-facing nor publicly accessible?		
2.	Does external entity policy require use of strong password controls by external entity employees[5], independent contractors, subcontractors and temporary employees that include instructions on how to: a) Choose effective passwords? b) Protect passwords? c) Change and store passwords and PINs?		
Additional Comments:			

[5] The term "external entity employees" means full-time and part-time employees of external entity.

2.6 Business Continuity Management

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
1.	Does external entity policy establish requirements for the development, maintenance and testing of the following: a) Emergency response? b) Disaster recovery? c) Business continuity practices?		
Additional Comments:			

2.7 Compliance

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
1.	Does external entity policy require appropriate treatment by external entity of the following information assets that reside on external entity, customer and/or third-party systems to which external entity may be provided access in connection with the provision of the services: a) Personally identifiable education records? b) PIFI/ePIFI? c) PCI/ePCI? d) PHI/ePHI?		
2.	Does external entity policy require timely and efficient reporting of and response to information security incidents?		
3.	Does external entity maintain a detailed incident response plan that: a) Defines roles and responsibilities? b) Establishes procedures detailing actions taken during the incident based on: a. Incident type (e.g., virus, hacker intrusion, data theft, system destruction)? b. Severity of threat to system or data? c. Status of incident (e.g., active, contained)?		
4.	Does external entity policy provide requirements for external entity employees, independent contractors, subcontractors and		

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
	temporary employees to notify identified contacts internally in the event of suspected unauthorized access to: a) Customer data? b) Personally identifiable education records? c) PIFI/ePIFI? d) PCI/ePCI? e) PHI/ePHI?		
Additional Comments:			

3.0 Physical Security Safeguards

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
1.	Do external entity physical security standards restrict access to service locations to only the following: a) External entity employees? b) Independent contractors and subcontractors? c) Temporary employees? d) Authorized visitors?		
2.	Do external entity standards require that identification cards be issued to and worn while on the premises by the following individuals: a) External entity employees? b) Independent contractors and subcontractors? c) Temporary employees? d) Authorized visitors?		
3.	Do external entity standards require authorized visitors to adhere to the following guidelines when on the premises: a) Sign a visitor's register? b) Be escorted and/or observed? c) Enter into a written confidentiality agreement with external entity?		

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
	d) Return external entity-issued identification cards upon departure?		
4.	Do external entity standards require external entity security to monitor: a) Possession of keys/access cards? b) Ability to access service locations?		
5.	Do external entity standards require: a) Keys/cards to be returned by staff leaving external entity's employment? b) Keys/cards to be deactivated upon termination? c) After-hours access to service locations to be monitored and controlled by external entity security? d) All repairs and modifications to the physical security barriers and/or entry controls at service locations to be authorized by external entity security?		
Additional Comments:			

4.0 Network Security

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
1.	Does external entity policy employ intrusion prevention and detection systems within the external entity network to provide continuous surveillance: a) For intercepting and responding to security events? b) In real time as security events are identified? c) By using a network-based monitoring approach to detect attacks on open ports? d) By using signature detection to match patterns of environment settings and user activities against a database of known attacks? e) By updating the signature database as new releases become available for commercial distribution?		

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
	f) For dispatching alerts to external entity's personnel who will review and respond to potential threats?		
2.	Does external entity policy require use on the external entity network of: a) Access control lists? b) Segmentation to separate customer data?		
3.	Do external entity standards require: a) Management and monitoring by external entity's IT department of all routers and firewall logs? b) Safeguarding of network devices via centralized authentication? e) Auditing of network usage?		
4.	Do external entity standards require external entity to access the environments residing on customer's system over the Internet by using either of the following technologies: a) Encrypted network traffic via another industry standard Virtual Private Network (VPN) or equivalent technology? b) Technology permitted by customer's network administrator?		
Additional Comments:			

5.0 Data Management/Protection

5.1 Deletion of Environments

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
1.	Does external entity policy require that upon termination of services or at customer's request, external entity will: a) 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? b) Archive environments on tape for six		

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
	(6) months following termination of the services, unless otherwise specified in writing by customer or by judicial or regulatory order?		
Additional Comments:			

5.2 Reporting Security Incidents

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
1.	Does external entity policy require that if the customer 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: a) External entity will frequently evaluate and respond to incidents that create suspicions of unauthorized misappropriation of customer's data, and 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? b) If external entity determines that data in customer's environment(s) may be or has been subject to a legal determination that a security incident has occurred (including by a external entity employee) or any other circumstance in which customer is required to provide a notification under applicable law, external entity will, unless otherwise required by law, report within 24 hours such misappropriation in writing to customer's privacy officer?		
2.	Does external entity policy require that external entity personnel be instructed in addressing incidents where handling of data has been misappropriated, including prompt and reasonable reporting and escalation procedures?		
Additional Comments:			

5.3 Disclosure of Data

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
1.	Does external entity policy prohibit external entity from disclosing data located on external entity, customer and/or third-party systems to which external entity may be provided access in connection with the provision of the services, including text and images, except in accordance with customer's contract, customer's written instructions, or to the extent required by law?		
2.	Does external entity policy require that external entity use diligent efforts to inform customer, to the extent permitted by law, of any request for such disclosure before disclosure is made?		
Additional Comments:			

6.0 Access Control

6.1 Account Provisioning and Passwords

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
1.	Does external entity policy require external entity to maintain the following standards for provisioning access to and creating passwords for the environments that are in the control of external entity: a) Access is provisioned on a need-to-know basis? b) Passwords conform to the strong password guidelines that include: a. Complexity? b. Expiration? c. Duplicity? d. Length? c) Passwords are neither written down nor stored on-line unencrypted in a reversible format? d) Passwords are treated as external entity confidential information? e) At customer's request, external entity will agree with customer on a schedule for periodic password changes? f) User IDs and passwords to customer's systems are not		

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
	communicated to any other person without customer's prior written authorization?		
Additional Comments:			

6.2 General Access

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
1.	Does external entity policy require in the event of employee terminations, deaths or resignations, external entity will take actions to terminate network, telephony and physical access for such former employees?		
2.	Does external entity policy require that external entity security frequently review accounts of terminated employees to verify that access has been terminated and that stale accounts have been removed from external entity's network?		
Additional Comments:			

7.0 Additional External Entity Practices

7.1 Computer Virus Controls

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
1.	Does external entity policy require external entity to maintain mechanisms within the external entity network for computers issued to external entity employees, independent contractors, subcontractors and temporary employees and with the following capabilities: a) Scans email sent both to and from any external entity recipient/sender for malicious code? b) Deletes email attachments that are infected with known malicious code prior to delivery?		
2.	Does external entity policy require all external entity employee, independent contractor, subcontractor and temporary employee laptops to be equipped with virus protection software?		
3.	Does external entity policy require external entity to maintain mechanisms that ensure: a) Virus definitions are frequently updated? b) Updated definitions are published and communicated to external entity		

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
	employees, independent contractors, subcontractors and temporary employees? c) External entity employees, independent contractors, subcontractors and temporary employees are able to automatically download new definitions and update virus protection software? d) Compliance reviews are frequently conducted by external entity?		
4.	Does external entity policy require all customer data stored on external entity employee, independent contractor, subcontractor and temporary employee laptops and removable media be encrypted?		
Additional Comments:			

7.2 Information Security Managers

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
1.	Does external entity policy establish the "Information Security Manager" role under which an advocate within external entity has the following responsibilities: a) Communicate information security awareness to external entity employees, independent contractors, subcontractors, temporary employees and management? b) Work effectively with external entity employees, independent contractors, subcontractors, temporary employees and management to help implement and comply with external entity's corporate security practices, policies and initiatives?		
Additional Comments:			

8.0 Human Resources Security

8.1 Personnel

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
1.	Does external entity code of ethical conduct require compliance with and acknowledgement of it by the following: a) External entity employees?		

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
	b) Independent contractors? c) Subcontractors? d) Temporary employees?		
2.	Does external entity code of ethical conduct stress reduction of the following risks: e) Human error? f) Theft? g) Fraud? h) Misuse of facilities?		
3.	Do external entity's efforts include: a) Personnel screening? b) Making personnel aware of security policies? c) Training employees to implement security policies?		
Additional Comments:			

8.2 Security Requirements

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
1.	Does external entity policy require external entity employees, independent contractors, subcontractors and temporary employees to take the following measures to protect the security of the environments: a) Adhere to written confidentiality agreements? b) Comply with company policies concerning protection of confidential information? c) Store materials containing data securely and share those materials internally only for the purposes of providing the services? d) 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 (if shredders are available at client site)?		

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
Additional Comments:			

8.3 Independent Contractors and Subcontractors

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
1.	Does external entity policy require that external entity enter into the following written agreements with each independent contractor and subcontractor: a) Confidentiality agreement? b) Services provider agreement that includes the external entity standards which require implementation of physical, technical and administrative safeguards consistent with external entity's obligations under the order and the *MCCCD External Entity Security and Hosting Standards and Practices* document? c) Network access agreement?		
2.	Does external entity policy establish that external entity is responsible for assuring that the independent contractors and subcontractors access, use and protect the security of the environments in a manner consistent with: a) The terms of the order? b) The *MCCCD External Entity Security and Hosting Standards and Practices* document?		
Additional Comments:			

8.4 Training

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
1.	Does external entity policy establish that all external entity employees, independent contractors, subcontractors and temporary employees complete online information protection awareness training that satisfies the following requirements: a) Conducted upon hiring and at least every two years thereafter? b) Instructs participants on their obligations under the various central external entity privacy and security policies?		

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
	c) Instructs participants on data privacy principles and data handling practices that may apply to their jobs at external entity and are required by company policy, including those related to: a. Notice? b. Consent? c. Use? d. Access? e. Integrity? f. Sharing? g. Retention? h. Security? i. Disposal?		
2.	Does external entity policy require that external entity: a) Perform periodic compliance reviews to determine if external entity employees, independent contractors, subcontractors and temporary employees have completed the online information protection awareness training course? b) Promptly notify and instruct external entity employees, independent contractors, subcontractors and temporary employees to complete training, if external entity determines they have not done so? c) Prepare and distribute written materials to promote awareness about security-related issues?		
Additional Comments:			

8.5 Enforcement

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
1.	Does external entity policy establish that: a) External entity conduct security reviews, assessments and audits frequently to confirm compliance with external entity information security policies, procedures		

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
	and practices? b) External entity employees, independent contractors, subcontractors and temporary employees who fail to comply may be subject to disciplinary action, up to and including termination? c) External entity provide customer with a copy of the results of the security reviews, assessments, and audits within one week of either positive or negative results? d) If external entity materially fails a review, assessment and/or audit or is unable to execute an agreed-to remediation plan, customer may terminate the contract and any further payment obligation?		
Additional Comments:			

MCCCD EXTERNAL ENTITY SECURITY AND HOSTING PRACTICES AND STANDARDS

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

I. Definitions

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

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

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

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

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

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

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

II. Security Policies

External Entity’s corporate security policies must cover the management of security for both its internal operations as well as the Services External Entity provides to its customers, and apply to all External Entity employees, subcontractors and third-parties to External Entity, temporary employees, and individuals and legal persons that

are involved in delivering services. These policies, which are aligned with the ISO/IEC 17799:2005 and ISO/IEC 27001:2005 standards, govern all areas of security applicable to the services.

Organizational Security

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

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

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

Asset Classification and Control

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

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

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

Human Resource Security

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

Physical and Environmental Security

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

Access Control

- External Entity should have a policy that describes logical access control requirements for all external entity systems, including authentication, authorization, access approval, provisioning, and revocation for employees and any other external entity-defined 'users' with access to external entity systems which are not Internet facing publicly accessible systems.
- External Entity should have a policy that requires protection of information assets by external entity employees, through the use of strong password controls where passwords are being used as a method of authentication.

- External Entity's policy should describe the identity and access management method to define, allocate, adjust or remove an identity. The policy should address the characteristics of an identity, so as to ensure each identity is unique

Business Continuity Management

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

Compliance

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

III. Physical Security

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

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

IV. Network Security

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

- External Entity employs intrusion detection systems within the External Entity network to provide continuous surveillance for intercepting and responding to security events as they are identified. External Entity utilizes a network-based monitoring approach to detect attacks on open firewalls ports within External Entity's network. Events are analyzed using signature detection, which is a pattern matching of Environment settings and user activities against a database of known attacks. External Entity updates the signature database as new releases become available for commercial distribution. Alerts are forwarded to External Entity's IT department for review and response to potential threats.
- External Entity uses router rules, access control lists and segmentation on the External Entity network.
- External Entity's IT department manages and monitors all routers and firewall logs. Network devices are safeguarded via centralized authentication; usage is audited.
- When External Entity accesses the Environments residing on MCCCD's system over the Internet, it uses only (a) encrypted network traffic via industry standard Virtual Private Network (VPN) or equivalent technology, or (b) technology permitted by MCCCD's network administrator (e.g., direct dial-up or DSL if permitted on MCCCD's network). Unless otherwise specified in MCCCD's order, in (a) above, External Entity uses External Entity Continuous Connection Network (OCCN), which utilizes a persistent VPN tunnel and Cisco Software VPN Combination, for internet-based connections to the Environments.

- To the extent specified in MCCCD's order, External Entity may also use a desktop/laptop client based product when it accesses the Environments residing on MCCCD's system over the Internet. Examples include: Cisco Software VPN, Nortel Software VPN, Checkpoint Software VPN, Netscreen Software VPN, Point-To-Point Tunneling Protocol (PPTP), Neoteris Secure Sockets Layer (SSL) VPN, Aventail SSL VPN.
- External Entity shall ensure that all systems that contact MCCCD's network are controlled and managed from a virus protection perspective, to the extent that unmonitored or unwarranted systems (i.e. BYOD without External Entity Device Image) will be prohibited from connecting to MCCCD's network.

V. Data Management/Protection

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

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

- External Entity will promptly evaluate and respond to incidents that create suspicions of unauthorized misappropriation of MCCCD's data. External Entity security will be informed of such incidents and, depending upon the nature of the activity, will define escalation paths and response teams to address the incidents.
- If External Entity determines that data in MCCCD's Environments has been misappropriated (including by a External Entity employee), External Entity will report such misappropriation to MCCCD in writing.
- External Entity personnel are instructed in addressing incidents where handling of data has been misappropriated, including prompt and reasonable reporting and escalation procedures.

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

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

VI. Access Control

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

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

General Access: In the event of employee terminations, deaths or resignations, External Entity will take immediate actions to terminate network, telephony and physical access for such former employees. External

Entity security will periodically review accounts of terminated employees to verify that access has been terminated and that stale

VII. Additional External Entity Practices

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

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

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

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

VIII. Human Resources Security

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

Employee Security Requirements

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

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

Subcontractors

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

Employee Training

- All External Entity employees are required to complete information protection awareness training upon hiring and at least every two years thereafter. The course instructs employees on their obligations under the various central External Entity privacy and security policies. The course also trains employees on

data privacy principles as well as data handling practices that may apply to their jobs at External Entity and are required by company policy, including those related to notice, consent, use, access, integrity, sharing, retention, security and disposal of data.

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

Enforcement

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

VII. Additional External Entity Practices

Computer Virus 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 MCCCD network to be loaded with virus protection software. External Entity maintains mechanisms to ensure that virus definitions are regularly updated on all devices, and that updated definitions are published and distributed to employee devices per direct.. 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.

CONTRACT TERMS

The following list provides examples of topics for security and privacy contractual terms that MCCCD External Entities may be asked to adopt:

Background Check and other Personnel Policies

Confidential Information

Cybersecurity Insurance

Dispute Resolution

Hosting Location

Maintenance and Incorporation of Privacy and Security Policies

Mitigation of Effect of Security Incident

Notification of Security Incident

Personnel Policies

Privacy Laws

Record and Data Retention, Ownership and Decommissioning

Termination for Breach