# **REQUEST FOR PROPOSAL (RFP) TEMPLATE**

**Instructions for Using the RFP Template**

* This RFP template has been completely revised to accommodate the new business processes initiated as a result of implementing the State Procurement Bureau’s electronic procurement system, eMACS. The sections that were defined in the old paper RFP process have been removed. All that is left are the particular clauses that require decisions to be made by the agency.
* Instructions to agencies appear in **blue**.
* Insert appropriate information when requested in areas that appear in **red**.
* Decide which optional paragraphs are needed and delete those not needed.
* If you are preparing an IT RFP, be sure to include all language specific to IT projects.
* Include a copy of the contract you intend to use.
* For all solicitations for which Prevailing Wage Rates will be paid, the applicable Prevailing Wage Booklet from the Department of Labor and Industry must be included as part of the solicitation. Current Prevailing Wage Booklets are available at the [Department of Labor and Industry Website](http://erd.dli.mt.gov/labor-standards/state-prevailing-wage-rates).
* Call the State Procurement Bureau with questions at 444-2575.

**Tips for fillable WORD documents:**

1. When you click on the text and see Click to Delete, you can select the word or sentence to delete.



1. You will also have the option to click on the text and enter the appropriate information.



**SCHEDULE OF EVENTS**

|  |  |
| --- | --- |
| **EVENT** | **DATE** |
| Pre-Proposal Conference (Optional) |  |
| Deadline for Receipt of Written Questions |  |
| Deadline for Posting Written Responses to the State's Website |  |
| RFP Response Due Date |  |
| Notification of Offeror Interviews/Product Demonstrations (Optional)\* |  |
| Offeror Interviews/Product Demonstrations (Optional)\* |  |
| Intended Date for Contract Award (Optional)\* |  |
| \*The dates above identified by an asterisk are included for planning purposes. These dates are subject to change. | |

Pre-Proposal Conference is optional. Customize for Conference or Conference Call. Carefully consider the consequences of making this requirement mandatory.

**Pre-Proposal Conference**

A(n) mandatory/optional Pre-Proposal Conference/Conference Call will be conducted at insert address on insert date at insert time. Offerors are encouraged to use this opportunity to ask clarifying questions, obtain a better understanding of the project, and to notify the State of any ambiguities, inconsistencies, or errors discovered upon examination of this RFP. All responses to questions during the Pre-Proposal Conference/Conference Call will be oral and in no way binding on the State. Proposal responses from any offeror failing to participate in the Pre-Proposal Conference/Conference Call will not be considered.

If conducting a conference call, add the following sentence.

If calling from the Helena area, call (406) 444-insert.If calling from outside the Helena area, call insert number. The password for both numbers is insert.

The following sections are to be used for IT RFPs only.

**Department of Administration Powers and Duties**

The Department of Administration is responsible for carrying out the planning and program responsibilities for information technology (IT) for state government. (Section 2-17-512, MCA). The Chief Information Officer is the person appointed to carry out the duties and responsibilities of the Department of Administration relating to information technology. The Department of Administration shall:

Review the use of information technology resources for all state agencies;

Review and approve state agency specifications and procurement methods for the acquisition of information technology resources; and

Review, approve, and sign all state agency IT contracts and shall review and approve other formal agreements for information technology resources provided by the private sector and other government entities.

**Compliance with State of Montana IT Policies and Standards**

The offeror is expected to be familiar with the State of Montana IT environment. All services and products provided as a result of this RFP shall comply with all applicable State of Montana IT policies and standards in effect at the time the RFP is issued. If offeror cannot comply with any *applicable* Policy or Standard, it must request an exception by posting the requested changes to the Q&A Board by the deadline set for question submittal. It will be the responsibility of the State to deny the exception request or to seek a policy or standards exception through the State CIO.

The links below provide information on State of Montana IT strategic plans, current environment, policies, and standards.

State of Montana Information [Technology Strategic Plan](http://sitsd.mt.gov/Governance/IT-Plans)

State of Montana Information [Technology Environment](http://sitsd.mt.gov/Services-Support/Enterprise-Architecture)

State of Montana [IT Policies](https://sitsd.mt.gov/Governance/IT-Policies)

**State of Montana Approved Enterprise Software List (List)**

If an Offeror proposes to use third party software, the proposed software must meet the requirements of the List. The List will be made available to Offeror upon request to the Procurement Officer. Offeror’s failure to request the List does not release it from complying with all the requirements of the List.

**SUPPLY SPECIFICATIONS OR SCOPE OF SERVICES**

To enable the State to determine the capabilities of an offeror to provide the supplies and/or perform the services specified in the RFP, the offeror shall respond to the following regarding its ability to meet the State's requirements.

**NOTE**: Each item must be thoroughly addressed. Offerors taking exception to any requirements listed in this section may be found nonresponsive or be subject to point deductions.

Mandatory Requirements are optional and should be used with caution and only when absolutely necessary. All mandatory requirements must be clearly identified, listed here. A mandatory requirement is a particular condition or item that *must* be present for the proposal to be responsive, e.g. proof of licensure. Typically, a mandatory requirement is not an evaluation criterion.

**Mandatory Requirements**

To be eligible for consideration, an offeror *shall* meet all mandatory requirements noted herein. The State will determine whether an offeror's proposal complies with the requirements. Proposals that fail to meet any mandatory requirements listed in this RFP will be deemed nonresponsive.

**This section is the core of the RFP**. It delineates in detail what the agency is seeking the offeror to include in their proposal in terms of the specifications and/or requirements necessary for the project.

As you begin, ask yourself the following questions:

SMART

* Specific – Are the requirements for both the offeror and the State clear enough so they can only be interpreted in one way by everyone who reads the requirements?
* Measurable – What criteria will be applied to the requirements to ensure they are met?
* Achievable – Can it be done?
* Realistic – Can it be done given our constraints – are you willing to pay the price for this solution as written?
* Traceable – Is the requirement linked to the initial need of the customer, from conception through any changes and tests, on to implementation?

Use these suggestions and tips to help develop your Scope of Services or Supply Specifications:

Explain your reason or need for the service or supply. Give an overview and the background of the project.

1. Use affirmative action words only if you mean them (will, shall, must); don't use "would, should, may, or please". Avoid the use of jargon and vague references such as "prepared to our satisfaction" or "in a timely manner"; and "et cetera."
2. Explain what work is to be performed.
3. If possible, divide the contractor services or supplies into billable tasks or units.
4. What are the contractor's responsibilities?
5. What are the agency's responsibilities?
6. Address the level of interaction/oversight you anticipate for the project and the performance standards you expect.
7. Describe any overlapping duties and responsibilities between agency and contractor.
8. Specify what to do in the event third parties or subcontractors are involved.
9. What is the project timeline and/or the deadlines for deliverables? Is there more than one deadline date?
10. Are meetings required? What is the frequency? Must they be face-to-face?
11. If reports are required, when do you want them, in what format?
12. What performance standards will be used? Will third-party metrics be applied?
13. What will be the method of acceptance?
14. What is the final product you expect when work is completed? Or what do you expect as an outcome of the project?
15. Describe regulations and laws the contractor must follow, or licenses that are required.
16. How will problems be communicated and resolved?
17. How often will the agency pay? Will it be based on the percentage of work completed?
18. Clearly specify all mandatory requirements.
19. Do you have an established Information Security Program, including an Incident Response process? Your response should refer, where applicable, to the title of the employee in charge of the program, the number of employees in the program, any credentials or special skills, your organization’s incident response program, and security policies or procedures.
20. Do you have any certifications for any compliance frameworks such as FISMA, HIPAA, PCI, etc.? If custom application developed, describe any security frameworks (e.g., OWASP) used or formal processes (e.g., SDLC) in place.
21. Describe the controls your firm has in place to address the threat of information being compromised by an external hacker or malicious software. Response should refer, where applicable, to safeguards such as intrusion detection; antivirus; firewalls; vulnerability scanning; penetration testing; encryption; authentication; and authorization protections and policies, including those involving system hardening, such as passwords, removal of unnecessary network services, limiting of administrative access, code review, logging, employee training, and other relevant safeguards.
22. Describe controls to address the threat of information being intercepted in transit by unauthorized persons. Your response should refer where applicable to safeguards such as encryption during transmission, availability and/or encryption of wireless traffic, physically securing devices in transit, network traffic segregation, and other relevant safeguards, and include descriptions of encryption protocols and algorithms used.
23. Describe controls to address the threat of information being mistakenly disclosed to unauthorized persons. Your response should refer where applicable to issues of awareness and training, removal of unnecessary data (electronic and paper), use of screen savers and lockouts, limiting storage of confidential data on remote devices, verification of identity of individuals requesting access, and other relevant safeguards that enforce “need to know”.
24. Describe controls to address the threat of information knowingly being misused by your workforce and contractors. Your responses should refer, where applicable, to issues of strong sanctions policy and practice, background checks, role-based access to information, oversight of data authorization by

supervisor, terminating access to data for terminated employees and employees changing job functions, prohibition on sharing passwords, and other relevant safeguards.

1. Describe controls to address the threat of physical theft or loss of data. Your responses should refer, where applicable, to policies on the storage of confidential data on laptops, PDAs, USB drives and other portable devices, encryption of data on portable devices, two factor authentication, removal of unnecessary information, physical protection of desktops and servers, and other relevant safeguards.
2. Describe controls to address community concerns regarding privacy practices. Your responses should refer where applicable to privacy statements, opt-in or opt-out consents, compliance with applicable privacy rules, and other relevant safeguards.
3. Describe controls to address the use, handling, protection and sharing of confidential data shared with subcontractors. Your responses should state any relevant relationships that may induce additional risk to the safe storage of sensitive data (such as outsourcing of key services, use of sub-contractors or cloud services for hosting, etc.), and refer, where applicable, to contractual safeguards and reviews of security programs/practices.
4. Describe controls to address threats to the availability of data based on inadequate business continuity procedures. Your responses should refer to business continuity, disaster recovery plans and procedures, regular testing, routine data backups, and offsite storage.

Use the heading appropriate to your project.

Ability to Meet Supply Specifications.

OR

Provision of Services.

**OFFEROR QUALIFICATIONS**

To enable the State to determine the capabilities of an offeror to provide the supplies and/or perform the services specified in the RFP, the offeror shall respond to the following regarding its ability to meet the State's requirements.

**NOTE:** Each item must be thoroughly addressed. Offerors taking exception to any requirements listed in this section may be found nonresponsive or be subject to point deductions.

The following questions are examples that need to be tailored for each RFP. The Equal Pay for Montana Women MUST be included in all RFPs.

Use this section if you want references to be evaluated on a pass/fail basis.

**References**

Offeror shall provide a minimum of insert number references that are currently using or have previously used supplies and/or services of the type proposed in this RFP. The references may include state governments or universities for whom the offeror, preferably within the last insert number years, has successfully completed insert language pertaining to this type of contract. At a minimum, the offeror shall provide the company name, location where the supplies and/or services were provided, contact person(s), contact telephone number, e-mail address, and a complete description of the supplies and/or services provided, and dates of service. These references may be contacted to verify offeror's ability to perform the contract. The State reserves the right to use any information or additional references deemed necessary to establish the ability of the offeror to perform the contract. Negative references may be grounds for proposal disqualification.

OR

Use this section if you want references to be numerically scored. If you choose to request a written reference, there are optional forms available at the [State Procurement Website](http://spb.mt.gov/Procurement-Guide). Choose the form that works the best for your application and tailor it to fit your needs.

**Client Reference Form**

Offeror shall provide complete and separate Client Reference Form (found in prerequisites or buyer attachment), for insert number references that are currently using or have previously used supplies and/or services of the type proposed in this RFP. The references may include state governments or universities for whom the offeror, preferably within the last insert number years, has successfully completed insert language pertaining to this project. A responsible party of the organization for which the supplies and/or services were provided to the client (the offeror's customer) must provide the reference information and must sign and date the form. It is the offeror's responsibility to ensure that the completed forms are submitted with the proposal by the submission date, for inclusion in the evaluation process. Any Client Reference Forms that are not received or are not completed may adversely affect the offeror's score in the evaluation process. Client Reference Forms exceeding the specified number will not be considered. The State may contact the client references for validation of the information provided in the Client Reference Forms. If the State finds erroneous information, evaluation points may be deducted, or the proposal may be rejected.

**Company Profile and Experience**

Offeror shall provide documentation establishing the individual or company submitting the proposal has the qualifications and experience to provide the supplies and/or services specified in this RFP, including, at a minimum:

* a detailed description of any similar past projects, including the supply/service type and dates the supplies and/or services were provided;
* the client for whom the services were provided; and
* a general description of the firm including its primary source of business, organizational structure and size, number of employees, years of experience performing services similar to those described within this RFP.

**Resumes**

A resume or summary of qualifications, work experience, education, and skills must be provided for all key personnel, including any subcontractors, who will be performing any aspects of the contract. Include years of experience providing services similar to those required; education; and certifications where applicable. Identify what role each person would fulfill in performing work identified in this RFP.

The following option should be used *only in very limited circumstances*, depending on the nature of the project and needs to be tailored accordingly. If this information is requested, agencies must be prepared to have a qualified financial staff member evaluate it, typically on a pass/fail basis.

**Offeror Financial Stability**

Offerors shall demonstrate their financial stability to insert appropriate language specified by: (1) providing financial statements, preferably audited, for the insert number consecutive years immediately preceding the issuance of this RFP; and (2) providing copies of any quarterly financial statements that have been prepared since the end of the period reported by its most recent annual report.

Examples of service organizations are insurance and medical claims processors, trust companies, hosted data centers, application service providers, managed security providers, credit processing organizations, and clearinghouses.

**Service Organization's Internal Control Assessment**

Offerors shall provide a copy of the most recent independently conducted internal control assessment. This assessment should include review of accounting systems, IT security systems, and other transaction-based processes. Provide internal policy for ensuring these reviews are conducted on a regular schedule.

**ORAL PRESENTATION/PRODUCT DEMONSTRATION/INTERVIEW**

Oral Presentations/Product Demonstrations/Interviews are optional. If oral presentations are to be conducted as part of the evaluation, they must be scored, and the evaluation criteria must be listed in this RFP.

Consider listing offeror's staff that would be required to attend. Select ONE option from the list below:

Offerors must be prepared to have the key personnel assigned to this project complete a(n) oral presentation/product demonstration/interview in insert location, Montana. The State reserves the right to:

1. have presentations/demonstrations/interviews from only the insert number highest scoring offerors;
2. have presentations/demonstrations/interviews from all offerors within (insert percentage) of the highest scoring offeror; or
3. have presentations/demonstrations/interviews from all offerors who are deemed to have a passing score prior to the presentations/demonstrations/interviews process, at the State's discretion.

Tailor the following to fit the project needs.

Offerors selected to participate in oral presentations/product demonstrations/interviews will be notified by the State in advance. For planning purposes, the State will submit an agenda and specific guidance as deemed appropriate to promote productive and efficient oral presentations/product demonstrations/interviews.

Offerors will be required to bring certain key personnel to the oral presentations/product demonstrations/interviews. The following key staff must be present at a minimum. If the offeror is proposing to have a key staff member filling more than one position that information must be clearly addressed at the time of the oral presentations/product demonstrations/interviews on how staff will produce and perform all of the required functions, activities and deliverables for the combined job duties. Dual accountability, security issues and deadlines cannot be compromised. Offerors are welcome to bring additional staff at their discretion.

1. Account Manager
2. Project Manager
3. Operations Manager
4. Software Development Lead
5. Testing Lead
6. Training Lead
7. Customer Service Manager

The State reserves the right to schedule and conduct interviews with offerors’ proposed key staff following the oral presentations if in the best interest of the State.

**COST PROPOSAL**

If possible, include the estimated budget for the project so that the offeror can provide a realistic cost proposal within that range. For guidance in determining how to evaluate cost, please see examples in the RFP Manual and read the State Procurement Bureau resource document entitled "Cost Evaluation Methods for Requests for Proposals." Both are available at the [State Procurement Website](http://spb.mt.gov/Procurement-Guide).

Some items you may want to consider when developing this section are:

1. How do you want costs presented?
2. Itemized Budget with narrative justification
3. Total Project Cost
4. Task Order Basis (hourly rates)
5. eMACS provides cost line items for both products and services. Each of these can be further divided by groups, allowing for separation of project phases, product groupings, or optional items.
6. How do you want to be invoiced? How often, e.g. monthly, per deliverable, etc.? How much detail do you want, e.g. timesheets, subcontractor expenditures, supply invoices, etc.?
7. Do you need to know their accounting methods?
8. Is there a maximum amount? If so, include a statement that exceeding the maximum amount will disqualify the response from further consideration and list it as a mandatory item. A response cannot be disqualified for exceeding a budget ceiling unless that is stated in the RFP.
9. When drafting the cost matrix, consider all initial and potential future costs such as enhancements, additional features, ongoing maintenance costs, renewals, etc. You may want to request estimated costs for future years of the contract to have a clearer picture of the total contract value. If appropriate, this may be reflected in the cost section of the contract.

Price Sheets are optional. A sample price sheet can be found in the RFP Manual at the State Procurement Website.

**Price Sheets**

Offerors *must* use the RFP Price Sheets provided. These price sheets serve as the primary representation of offeror's cost/price. Offeror should include additional information as necessary to explain the offeror's cost/price.

**EVALUATION PROCESS**

Following are two scoring approaches:

1. The first approach is based on tasks or requirements, easily defendable, and works very well for projects with an extensive list of criteria;
2. The second approach provides broader scoring assignments per guideline category which can result in wider point separation, but also requires more detailed defending comments to support the score assignments.

APPROACH 1

BASIS OF EVALUATION

The evaluator/evaluation committee will review and evaluate the offers according to the following criteria based on a total number of insert number points.

The Ability to Meet Supply Specifications OR Provision of Services, References (select the method for evaluating references based on the choice made earlier), Company Profile and Experience, Resumes, and Oral Presentation/Product Demonstration/Interview portions of the proposal will be evaluated based on the following Scoring Guide. The Financial Stability and/or Service Organization's Internal Control Assessment portion of the proposal will be evaluated on a pass/fail basis, with any offeror receiving a "fail" eliminated from further consideration. The Cost Proposal will be evaluated based on the formula set forth below.

SCORING GUIDE

In awarding points to each of the scored evaluation criteria, the evaluator/evaluation committee will consider the following guidelines:

*Exceeds Requirement* = 3 points: A response exceeds the requirement when it is a highly comprehensive, excellent reply that goes beyond the requirement of the RFP to provide added value. In addition, the response may cover areas not originally addressed within the RFP and/or include additional information and recommendations that would prove both valuable and beneficial to the agency. The response includes a full, clear, detailed explanation of how the solution fits the requirement. No errors in technical writing.

*Meets Requirement* = 2 points: A good response that fully meets the requirement and demonstrates and explains in a clear and concise manner a thorough knowledge and understanding, with no deficiencies noted regarding technical approach.

*Partially Meets Requirement* = 1 point: A fair response that minimally meets most of the requirement set forth in the RFP but may have one or more deficiency, such as typos. The offeror demonstrates some ability to comply or has explained partly how their solution fits the requirement.

*Failed to Meet Requirement* = 0 points: A failed response does not meet the requirement set forth in the RFP. The offeror has not demonstrated sufficient knowledge of the subject matter or has grossly failed to explain how their solution meets the requirement.

EVALUATION CRITERIA

The following are the relative weights for each evaluated section of this RFP and a sample scoring sheet showing the weighting/point assignments:

|  |  |
| --- | --- |
| Evaluated RFP Section | Weight (%)  (determines aggregate points) |
| Ability to Meet Supply Specifications | % |
| Requirement #1 | % |
| Requirement #2 | % |
|  |  |
| OR |  |
| Provision of Services | % |
| Task Element #1 | % |
| Task Element #2 | % |
|  |  |
| References | Pass/Fail |
| Complete contact information provided. | P/F |
|  |  |
| OR |  |
| Client Reference Forms | % |
| Client Reference #1 | % |
| Client Reference #2 | % |
| Client Reference #3 | % |
|  | % |
| Company Profile and Experience | % |
| Years in Business | % |
| Relevant Experience | % |
| Relevant Past Projects | % |
|  |  |
| Resumes | % |
| Key Personnel | % |
|  |  |
| Financial Stability | Pass/Fail |
| Financial Stability | P/F |
|  |  |

|  |  |
| --- | --- |
| Equal Pay for Montana Women | 5% of Bonus Points |
| Service Organization's Internal Control Assessment | Pass/Fail |
| Internal Control Assessment | P/F |
|  |  |
| Oral Presentation/Product Demonstration/Interview | 20% |
| Oral Presentation | % |
| Product Demonstration | % |
| Oral Interview | % |
|  |  |
| Cost Proposal | 20% |

NOTE TO AGENCIES:

Cost Proposal must constitute 20% or more of the total available points. Exceptions to this must be documented in writing and approved by the Procurement Officer. There are several formulas that can be used to score price/cost. The most common approach is as follows. For assistance with other scoring methods, please review the State Procurement Bureau resource document entitled "Cost Evaluation Methods for Requests for Proposals" available on the [State Procurement website](https://spb.mt.gov/Procurement-Guide) or contact the State Procurement Bureau. The Average Cost evaluation method requires consultation with the State Procurement Bureau before it can be used.

Lowest overall cost receives the maximum allotted points. All other proposals receive a percentage of the points available based on their cost relationship to the lowest. Example: Total possible points for cost are

200. Offeror A's cost is $20,000. Offeror B's cost is $30,000. Offeror A would receive 200 points. Offeror B would receive 134 points ($20,000/$30,000) = 67% x 200 points = 134).

Lowest Responsive Offer Total Cost x Number of available points = Award Points This Offeror's Total Cost

APPROACH 2

BASIS OF EVALUATION

The evaluator/evaluation committee will review and evaluate the offers according to the following criteria based on a total number of insert number points.

The Ability to Meet Supply Specifications OR Provision of Services, References (select the method for evaluating references based on the choice made earlier), Company Profile and Experience, Resumes, and Oral Presentation/Product Demonstration/Interview portions of the proposal will be evaluated based on the following Scoring Guide. The Financial Stability and/or Service Organization's Internal Control Assessment portion of the proposal will be evaluated on a pass/fail basis, with any offeror receiving a "fail" eliminated from further consideration. The Cost Proposal will be evaluated based on the formula set forth below.

Achieve Minimum Score is optional. Do not include the Cost Section in a minimum score.

**Achieve Minimum Score**

Any proposal that fails to achieve (insert number) % of the total available points for (identify the criterion) (or a total of (insert number) points)will be eliminated from further consideration. A "fail" for any individual evaluation criteria may result in proposal disqualification at the discretion of the procurement officer.

SCORING GUIDE

In awarding points to the evaluation criteria, the evaluator/evaluation committee will consider the following guidelines:

*Superior Response* (95-100%): A superior response is an exceptional reply that completely and comprehensively meets all of the requirements of the RFP. In addition, the response may cover areas not originally addressed within the RFP and/or include additional information and recommendations that would prove both valuable and beneficial to the agency.

*Good Response* (75-94%): A good response clearly meets all the requirements of the RFP and demonstrates in an unambiguous and concise manner a thorough knowledge and understanding of the project, with no deficiencies noted.

*Fair Response* (60-74%): A fair response minimally meets most requirements set forth in the RFP. The offeror demonstrates some ability to comply with guidelines and requirements of the project, but knowledge of the subject matter is limited.

*Failed Response* (59% or less): A failed response does not meet the requirements set forth in the RFP. The offeror has not demonstrated sufficient knowledge of the subject matter.

EVALUATION CRITERIA

NOTE TO AGENCIES: These categories need to be tailored to each project. These are only examples.

Identify the major criteria that are critical to the success of the RFP. In most cases, this should correspond to the Ability to Meet Supply Specifications or Provision of Services, References, Company Profile and Experience, and Resumes set out earlier. Some commonly used criteria are qualifications, relevant experience, quality of work, references, service, physical facilities, human resources, cost, technical capabilities, industry standards, and proposed timelines. RFPs can only be evaluated on stated criteria, so

include everything to be measured and ensure that the criteria are measurable. Once you have determined the major categories, reference those sections of the RFP that set out the specific criteria that will be evaluated and determine point assignments accordingly. Use the following as an example.

Insert or delete rows as necessary. In addition, this table may be used as a basis for score sheets. Copy and paste into a new document and insert columns on the right side for assigned scores and comments.

|  |  |
| --- | --- |
| Evaluated RFP Section | Point Values |
| Ability to Meet Supply Specifications | % of points for a possible points |
| Requirement #1 | X points |
| Requirement #2 | X points |
|  |  |
| OR |  |
| Provision of Services | % of points for a possible points |
| Methods | X points |
| Work Plan | X points |
| Timeline | X points |
|  |  |
| References | Pass/Fail |
| Complete contact information provided. | P/F |
|  |  |
| OR |  |
| Client Reference Forms | % of points for a possible points |
| Client Reference #1 | X points |
| Client Reference #2 | X points |
| Client Reference #3 | X points |
|  |  |
| Company Profile and Experience | % of points for a possible points |
| Years in Business | X points |
| Relevant Experience | X points |
| Relevant Past Projects | X points |
|  |  |
| Resumes | % of points for a possible points |
| Key Personnel | X points |
|  |  |
| Financial Stability | Pass/Fail |
| Financial Stability | P/F |
|  |  |

|  |  |
| --- | --- |
| Equal Pay for Montana Women | 5% of Bonus Points |
|  |  |
| Service Organization's Internal Control Assessment | Pass/Fail |
| Internal Control Assessment | P/F |
|  |  |
| Oral Presentation/Product Demonstration/Interview | % of points for a possible points |
| Oral Presentation | X points |
| Product Demonstration | X points |
| Oral Interview | X points |
|  |  |
| Cost Proposal | 20% of points for a possible points |
| Cost Proposal | X points |

NOTE TO AGENCIES: Cost Proposal must constitute 20% or more of the total available points. Exceptions to this must be documented in writing and approved by the Procurement Officer. There are several formulas that can be used to score price/cost. The most common approach is as follows. For assistance with other scoring methods, please review the State Procurement Bureau resource document entitled "Cost Evaluation Methods for Requests for Proposals" available at the [State Procurement Bureau Website](http://spb.mt.gov/Procurement-Guide.) or contact the State Procurement Bureau. The Average Cost evaluation method requires consultation with the State Procurement Bureau before it can be used.

Lowest overall cost receives the maximum allotted points. All other proposals receive a percentage of the points available based on their cost relationship to the lowest. Example: Total possible points for cost are

200. Offeror A's cost is $20,000. Offeror B's cost is $30,000. Offeror A would receive 200 points. Offeror B would receive 134 points (($20,000/$30,000) = 67% x 200 points = 134).

Lowest Responsive Offer Total Cost x Number of available points = Award Points This Offeror's Total Cost

**CONTRACT**

Include your agency contract or the most recent [SPB Standard Contract](http://spb.mt.gov/Procurement-Guide).

Be sure to select the appropriate file (non-IT or IT).

For IT solicitation be sure to choose the appropriate file (Services Contract, License Agreement, or SaaS Agreement).

The contract must be tailored to the project so only the appropriate clauses are included.

**MONTANA PREVAILING WAGE RATES FOR (INSERT TYPE OF SERVICE) SERVICES (YEAR)**

NOTE TO AGENCIES:

For all solicitations for which Prevailing Wage Rates will be paid, the applicable Prevailing Wage Booklet from the Department of Labor and Industry must be included as part of the solicitation. Current Prevailing Wage Booklets are available at the [Department of Labor and Industry website](http://erd.dli.mt.gov/labor-standards/state-prevailing-wage-rates). The booklet must be posted with the solicitation.

**SECURITY AND PRIVACY CONTROL REQUIREMENTS**

Through policy, the State of Montana’s Chief Information Officer (CIO) has determined that the State of Montana shall follow the National Institute of Standards and Technology (NIST) security guidelines and the Federal Information Security Management Act (FISMA). Any personally identifiable information from the system that is used by or available to the contractor, its employees, its subcontractors, and the employees of its subcontractors must be kept confidential and data shall only be shared in accordance with applicable interconnection security agreements, business associate agreements, computer matching agreements, and/or privacy protection agreements. The Contractor must comply with all requirements, as provided in the current revision of the [NIST SP 800-53](https://nvd.nist.gov/800-53), for a moderate impact system, and must provide annual assurance of such compliance.

The Contractor shall meet each of the security and system integrity requirements as referenced below:

1. The Bidder shall provide a description of relevant experience relating to the services/products requested in this IFB.

NOTE TO AGENCY: If this IFB is for Software OR Hardware please REMOVE Section 2 and 2.1-2.14. If this IFB is for Software as a Service (SaaS) or a Major Application INCLUDE Section 2 and 2.1-2.14

1. The Contractor shall create and maintain a formal system security plan that complies with all NIST SP 800-53 security requirements relating to a moderate impact system that, at a minimum:
   1. Is consistent with the State of Montana’s [enterprise architecture](https://sitsd.mt.gov/Services-Support/Enterprise-Architecture);
   2. Explicitly defines the authorization boundary for the system;
   3. Describes the operational context of the information system in terms of mission and business processes;
   4. Provides the security categorization of the information system, as established by the State, including supporting rationale;
   5. Describes the operational environment for the informational system and relationships with or connection to other information systems;
   6. Provides an overview of the security requirements for the system;
   7. Identifies any relevant overlays, if applicable;
   8. Identifies any specific statutory and/or regulatory requirements (above and beyond the requirements stated in the current version of the NIST SP 800-53 Moderate Baseline Controls), if applicable;
   9. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions;
   10. Is accepted by the authorizing official or designated representative prior to plan implementation;
   11. Is distributed to appropriate personnel;
   12. Is reviewed and updated, at least annually, or whenever changes to the information system/environment of operation occur; and
   13. Is protected from unauthorized disclosure and modification.
   14. Describes in detail the process and plans to update the application to stay current with platforms and infrastructure.
2. The Contractor shall provide identification and authentication requirements for the system and provide integration with State of Montana network technologies. If the proposed system is to be hosted outside of the state network, access control can be used through [OKTA Montana](https://okta.loginmt.com).
3. The Contractor shall provide the process used to notify customers of application downtime for both planned and unplanned outages.
4. The Contractor shall describe in detail if the proposed system utilizes remote access for management of the system. Awardee must describe plans to use enterprise approved mechanisms for remote access.
5. The Contractor’s proposed solution shall support Federal Information Processing Standards (FIPS) 140-2 compliant encryption.

NOTE TO AGENCY: If this IFB is for Software OR Hardware please REMOVE Section 7 and 7.1-7.2 If this IFB is for Software as a Service (SaaS) or a Major Application INCLUDE Section 7 and 7.1-7.2

1. The Contractor shall provide in detail a security incident response plan.
   1. The Contractor must report security incidents that occur on the [agency] information systems that may affect [agency] or the State of Montana systems to the [agency] Chief Information Officer OR the designee as directed by the [agency] within 24 hours of discovery.
   2. The Contractor must provide, in detail, incident reporting processes and how an incident will be communicated to customers during an incident.

NOTE TO AGENCY: If this IFB is for Software OR Hardware please REMOVE Section 3.8 If this IFB is for Software as a Service (SaaS) or a Major Application INCLUDE Section 3.8

1. The Contractor shall provide, in detail, a disaster recovery plan addressing the intended

recovery efforts for the proposed system and data.

NOTE TO AGENCY: If this IFB is for Software please REMOVE Section 9 If this IFB is for Software as a Service (SaaS) or a Major Application INCLUDE Section 9

1. The Contractor shall describe, in detail, auditable events to be employed that would support after-the-fact investigations of security incidents, ensure that audit logs are retained for seven years and be made available upon request to the State or investigators. Audit logs must establish the type of event that occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.
2. The Contractor shall provide for inspections, by State personnel, State designee, or regulatory bodies and provide access to information and the environment, upon receiving a reasonable request from the State.
3. The Contractor shall provide annual security awareness and applicable role-based training to all concerned staff members.

11.1 The Contractor shall provide the Contract Liaison with a description and proof of completion of the security training given to the Contractor’s staff that have direct or indirect access to the proposed system.

1. The Contractor shall provide an overview of security practices of the Contractor regarding secure application development.
2. The Contractor shall provide administrator documentation for the information system, system component, or information system service that describes:
   1. Secure configuration, installation, and operation of the system, component, or service;
   2. Effective use and maintenance of security functions/mechanisms; and
   3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions.
3. The Contractor shall provide user documentation for the information system, system component, or information system service that describes:
   1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;
   2. Methods for user interaction, which enable~~s~~ individuals to use the system, component, or service in a more secure manner; and
   3. User responsibilities in maintaining the security of the system, component, or service.

The Contractor shall provide documentation on how the proposed system can or cannot meet each of the **Privacy** requirements, as referenced below.

The system shall provide and the Contractor must document privacy protections that include:

Statements of purpose for the collection of personally identifiable information;

Data quality and integrity checks that provide for validation and verification of personally identifiable information;

Data minimization and retention checks that ensure personally identifiable information collected, used, and retained is relevant and necessary for the purpose for which it was originally collected.

Information about location of data storage, addressing requirements to keep all data in the United States.

Data collected by proposed system will remain under the ownership of State of Montana, and will be made available on request by [agency] or termination of contract.

The Contractor will not copy any State data obtained while performing services under this IFB to any media, including hard drives, flash drives, or other electronic devices, other than as expressly approved by [agency].

The Contractor shall return all data that is the property of the State of Montana in a format specified by the State.

The Contractor shall return all data to the State of Montana upon completion or termination of the contract.

The Contractor shall return all sensitive information received from the State or created/received by Contractor on behalf of the State in a manner that is documented and consistent with the State’s policy on sanitization of information system media (both digital and non-digital), with sanitization mechanisms that are commensurate with the classification or sensitivity of that information.

If the State agrees that return or destruction of confidential information is infeasible; Contractor shall extend the protections of this IFB and or subsequent contract to such confidential information and limit further uses and disclosures of such confidential information to those purposes that make the return or destruction infeasible, for so long as Contractor maintains such confidential information.

1. The Contractor shall provide notice of a loss or suspected loss of privacy data to the [agency] Chief Information Officer, or designee as directed by the agency, within 24 hours of loss or suspected loss.

***Physical Security Language***

Please use the following criteria in determining escorted versus unescorted Access:

There are three levels of access to the data centers – controlling access, escorted access and unescorted access.

Controlling access is given to employees who have unlimited access authority to the data centers.

1. Controlling Access is given to employees who have unlimited access authority to the Data Centers.
   1. Controlling Access is granted to the staff whose job responsibilities require that they have access to the area on a day-to-day basis. These individuals also have the authority to grant temporary access to a Data Center and to enable others to enter and leave a Data Center. People with Controlling Access are responsible for the security of the area, and for any individuals that they allow into a Data Center. Individuals with Controlling Access to a Data Center normally will be granted access via a cardkey and will be placed on the Data Center Access List. These individuals must wear their State Identification Card visibly at all times while in a Data Center. Any individual receiving Controlling Access must go through a formal background check according to their identified risk designation (see the Personnel Security Policy, Personnel Security Procedure, and Background Checks for Contractors, Lessees, and External Personnel Procedure).
   2. Individuals granted controlling access may, in addition to the cardkey they are issued, request key access. While it is not a best practice to issue keys to a Data Center for routine access purposes, requests for this type of access will be considered on a case-by-case basis.
   3. In addition to cardkey access, individuals granted controlling access will be required to gain physical access using two-factor authentication. Two-factor authentication uses biometrics in addition to the cardkey to provide access to some secured areas.
   4. Individuals with Controlling Access to an area may allow authorized and logged individuals Escorted or Unescorted Access to a Data Center.
   5. If a person with Controlling Access allows Escorted Access to an individual, the person granting access is responsible for escorting the individual granted access and seeing to it that they sign in and out on the access log. If needed, these duties can be handed-off to one of the staff that is on duty in a Data Center.
2. Escorted Access is closely monitored access given to people who have a legitimate business need for infrequent access to a Data Center. “Infrequent access” is generally defined as access required for less than 15 days per year.
   1. Individuals with Escorted Access will not be issued keys or be granted access via cardkey.
   2. A person given Escorted Access to an area must sign in and out on the access log under the direct supervision of a person with Controlling Access or Unescorted Access. They must also provide positive identification upon demand and must leave the area when requested to do so.
   3. A person given escorted access will be given a “Visitor” badge after they sign in, which must be worn visibly at all times.
   4. A person with Escorted Access to an area must not allow any other person to enter or leave the area.
3. Unescorted Access is granted to a person who does not qualify for Controlling Access but has a legitimate business reason for unsupervised access to a Data Center. An example of this would be a State Employee or Approved Vendor who requires access to work on their system for a set period of time.
   1. Individuals with Unescorted Access to a Data Center will be granted access to the area via cardkey. For additional process information regarding individuals with unescorted access, see the Temporary Badge Procedure.
   2. Persons with Unescorted Access should only enter a Data Center to perform tasks that cannot be performed remotely.
   3. Unescorted Access personnel cannot authorize others to be granted access to a Data Center. They must alert someone with Controlling Access that they will be escorting a Staff Employee or Approved Vendor that themselves do not have Data Center access.
   4. All individuals with Unescorted Access must wear their badge visibly at all times while in a Data Center.

**Data Center Doors**

1. All doors to a Data Center must remain locked at all times and may only be temporarily opened for periods not to exceed that minimally necessary in order to:
2. Allow officially approved and logged entrance and exit of authorized individuals.
3. Permit the transfer of supplies/equipment as directly supervised by a person with Controlling Access to the area. Internal and external doors will not be allowed to be opened at the same time except for cases where increased airflow is required (see item #3 below).
4. Doors to the Data Center will ONLY be propped open if it is necessary to increase airflow into the Data Center in the case of an air conditioning failure. In this case, staff personnel with Controlling Access must be present to limit and monitor access to the Data Center.

**Security System and Keys**

1. Keys to a data center are not generally issued for routine access purposes. The following information pertains to keys and the security system:
2. If a key is provided, the individual receiving the key may not share, loan or copy it.
3. Only those people who have been granted Controlling Access can request and be issued keys.
4. Under no circumstances may an individual attempt to bypass the cardkey system to gain access for them or permit access to another individual by using a key.
5. Individuals are not to share their cardkey.
6. If the biometric system being used fails, employees will be allowed into the facility by an employee with controlling access who can identify them. The accessing employee must show their cardkey to the employee with controlling access before entry into the secured facility will be allowed.

**Review and Removal of Access**

1. Monthly reviews will be performed of physical access to the Data Centers. If an individual no longer requires access to a Data Center or if the cardkey has been inactive for more than 90 days, the access will be removed.
   1. For Individuals whose access is removed for termination or no business need:
      1. In the Data Center Access List, they will be reclassified as “De-active”
      2. In the Bio-Metric system their fingerprint will be deleted
   2. For individuals whose access is removed because of inactivity for more than 90 days and they do not have a 90-day exception:

Notification will be sent to the individual whose access has been removed for inactivity for more than 90 days.

* + 1. In the Data Center Access list, they will be reclassified as Access – Inactive 90 days
    2. In the Bio-Metric system their fingerprint will be disabled.
    3. They can access the Data Center if their Authorization Granted in the Data Center Access List is less than three years old and no one has revoked their access. They will be issued an active visitor badge to perform their duties.
  1. -90-Day Exception Process:
     1. Any individual with cardkey and bio-metric access can ask to be part of the 90-Day exception group. Examples would be State Employees or Authorized Vendors needed for emergency response, Authorized Vendors that are contractually obligated to respond in a given time frame that may require access during unoccupied times of a Data Center.
     2. Requests must be submitted by a person’s supervisor if a State Employee or by the supervisor in charge of an Authorized Vendors contract.
     3. The request must be given to the ISB office for review by the CISO.

1. Periodic (at least annual) reviews will be performed on the location of keys to the Data Centers. If an individual no longer needs a key, it will be collected.
2. Procedures for removing access to a Data Center include:
   1. Canceling cardkey access
   2. Collecting a key
   3. Removing the person’s name from the Data Center Access List
3. The results of periodic reviews will be reported to the SITSD Information Systems Security Officer. The report will include an updated list of those allowed access to the Data Centers.

**Data Center Access List**

1. The Data Center Access List is managed by Data Center Facilities staff.
2. Individuals with Controlling Access to a Data Center (not just Data Center staff) are responsible for maintaining the Data Center Access List. The following procedures must be followed:
   1. Each time an individual with Escorted Access to a Data Center is admitted to an area, he/she must properly sign in on the Data Center Access List at the time of entrance.
   2. The person admitting the visitor must countersign and fill out the appropriate section of the form. The visitor must also present a picture identification card for verification of identity.
   3. Each time an individual with Escorted Access leaves the area, he/she must properly sign out on the Data Center Access List at the time of exit. NOTE: If an individual will be coming and going throughout the day, they can sign in and out one time for that day.
   4. The person escorting the visitor when they leave must fill out the “Time Out” section of the Sign in Sheet.

**Incident Reporting**

1. All infractions of the Data Center Physical Security Policies and Procedures shall be reported to the ISB. If warranted (e.g.: emergency, imminent danger, etc.) law enforcement should be notified as soon as is reasonably possible.
2. All high profile incidents will be reported to the SMDC Lead/Manager on site, the Manager-on-call, or the ISB immediately. Examples of high profile incidents are: an unauthorized individual in the Data Center, any attempt to enter a Data Center forcibly or improperly, missing or damaged equipment, etc.
3. Individuals with Controlling Access to the area are to monitor the area and have individual who appears to be compromising either the security of the area or its activities, or who is disrupting operations, removed. The State reserves the right to remove any contractor personnel who appear to be compromising the security. It is particularly important that individuals with Controlling Access show initiative in monitoring and maintaining the security of the Data Center.

**Requesting Access to the Data Centers**

1. All physical access to the Data Centers is granted according to group policy. Each person will be granted access according to the group for which they are associated.
2. **Contractors:**

2.1 Contract Administrators can request physical access for contractors to a data center. For process information on physical access and background checks for contractors, see the Physical Access Controls Procedure, and the Background Checks for Contractors, Lessees, and External Agency Personnel Procedure.

**Emergency Access**

If it becomes necessary to provide emergency access to medical, fire, and/or police officials, the escorted access procedure can be temporarily suspended.

**Other Information**

No camera or photographic equipment will be allowed within the Data Center without the approval of the SMDC Manager or ISB.