Attachment A

Mississippi Department of Education

Technical Requirements

School Based Administrative Claiming Support and Nurse Database Software Solution

[I. General 4](#_Toc201163109)

[A. How to Respond 4](#_Toc201163110)

[B. Overview and Background 4](#_Toc201163111)

[C. Procurement Goals and Objectives 5](#_Toc201163112)

[D. Glossary of Terms 5](#_Toc201163113)

[E. Statement of Understanding 5](#_Toc201163114)

[F. Hosting Environment 6](#_Toc201163115)

[G. Offeror Qualifications 9](#_Toc201163116)

[H. Offeror Implementation Team 10](#_Toc201163117)

[II. Functional/Technical Requirements 10](#_Toc201163118)

[A. Web Access 10](#_Toc201163119)

[B. Mobile Access 10](#_Toc201163120)

[C. User Interface and User Experience 11](#_Toc201163121)

[D. Functional/Technical 12](#_Toc201163122)

[E. Workflow 14](#_Toc201163123)

[F. Reports and Dashboards 14](#_Toc201163124)

[G. Notifications and Alerts 16](#_Toc201163125)

[H. Search Function 16](#_Toc201163126)

[I. Audit Function 17](#_Toc201163127)

[J. Archival 17](#_Toc201163128)

[K. Administrative Management 17](#_Toc201163129)

[L. Financial Management 18](#_Toc201163130)

[M. Calendar Function 18](#_Toc201163131)

[III. System/Solution Design 19](#_Toc201163132)

[A. Data Management 19](#_Toc201163133)

[B. Data Migration 19](#_Toc201163134)

[C. Backup Services 19](#_Toc201163135)

[D. Business Continuity/Disaster Recovery 20](#_Toc201163136)

[IV. Implementation Requirements 21](#_Toc201163137)

[A. Offeror Acknowledgement 21](#_Toc201163138)

[B. General Scope 21](#_Toc201163139)

[C. Compliance Standards 22](#_Toc201163140)

[D. Project Management Plan 22](#_Toc201163141)

[E. System Design Document 23](#_Toc201163142)

[F. Data Conversion and Migration 24](#_Toc201163143)

[G. Integrations and Interfaces 24](#_Toc201163144)

[H. User Acceptance Testing Plan 25](#_Toc201163145)

[I. User Training and Documentation 26](#_Toc201163146)

[J. Change Management and Control 26](#_Toc201163147)

[K. System Documentation 27](#_Toc201163148)

[L. Final Acceptance Review 27](#_Toc201163149)

[V. Software Administration and Security 27](#_Toc201163150)

[A. General 27](#_Toc201163151)

[B. Security Audit 28](#_Toc201163152)

[VI. Support and Maintenance 28](#_Toc201163153)

[A. Customer Support 28](#_Toc201163154)

[B. Issue Tracking 29](#_Toc201163155)

[C. Service Availability and Restoration 29](#_Toc201163156)

[D. System Monitoring 29](#_Toc201163157)

[E. System Availability Requirements 30](#_Toc201163158)

[F. Remedies for Failure to Meet Service Levels 31](#_Toc201163159)

[G. Patching 32](#_Toc201163160)

[H. Software/Product Updates 33](#_Toc201163161)

[I. Technology Refresh and Enhancements 33](#_Toc201163162)

[J. Change Order Rate 33](#_Toc201163163)

[VII. Deliverables 33](#_Toc201163164)

1. General
2. How to Respond
3. Beginning with Item 17, label and respond to each outline point in Attachment A as it is labeled.
4. The State is under the impression that Offerors have read and agree to all items in this RFP. Offerors should take exception to items to which they disagree.
5. The Offeror must respond with “WILL COMPLY” or “EXCEPTION” to each point in this section. In addition, many items in this RFP require detailed and specific responses to provide the requested information. Failure to provide the information requested will result in the Offeror receiving a lower score for that item or, at the State’s sole discretion, being subject to disqualification.
6. “WILL COMPLY” indicates that the Offeror can and will adhere to the requirement. This response specifies that a Offeror or Offeror’s proposed solution must comply with a specific item or perform a certain task.
7. If the Offeror cannot respond with “WILL COMPLY,” then the Offeror must respond with “EXCEPTION.” (See Exhibit B of the RFP, for additional instructions regarding Offeror exceptions.)
8. Where an outline point asks a question or requests information, the Offeror must respond with the specific answer or information requested.
9. In addition to the above, the Offeror must provide explicit details about how the proposal meets or exceeds each specification.
10. Overview and Background
11. The School Based Administrative Claiming Program offers school districts the opportunity to participate in a Medicaid reimbursement program that provides funding for normal, routine administrative duties performed within the school environment.
12. The Mississippi Department of Education (MDE) Office of Healthy Schools (OHS) is seeking a qualified software Offeror to provide:
    1. A Web-based random moment time study application based on the state plan methodology. The application will calculate administrative claims for participating school districts.
    2. A survey software solution that will enable MDE to collect, interpret, and analyze data provided by the school district nurses for reporting based on pre-formatted questions. The intent is to use the data to understand health and academic trends that may be used to measure the data summary reflected through monthly reporting.
13. Offeror must be able to design, develop, and deliver the applications as described in this Request for Proposal and in future meetings.
14. The current application is hosted by MDE in the MDE data center on a single Windows 2016 server. The application and database both reside on the server. The system is web-based and accessed by school district personnel, who maintain their district profiles.
15. Procurement Goals and Objectives
16. School Based Administrative Claiming Program Option goals and objectives:
17. The solution should replace the current system.
18. Keep accurate records based on federal and state requirements.
19. Provide accurate reporting
20. Provide a realistic timeline for transition.
21. Nurse Database application Option goals and objectives:
    1. The solution should replace the current system.
    2. Keep historical school year data and make it available as needed.
22. Glossary of Terms

|  |  |
| --- | --- |
| Glossary of Terms | |
| CMS | Centers for Medicare and Medicaid Services |
| Customer | Mississippi Department of Education (MDE) |
| ITS | Mississippi Department of Information Technology Services |
| Participant | School district employee who will be completing surveys. |
| Random Moment Time Study (RMTS) | A tool used by the School-Based Medicaid Program to measure what a person is doing during a moment of time of the workday. A specific date and time are chosen and assigned to a participant to identify what activity they are doing at that time. |
| SBAC | School-Based Administrative Claiming |
| State | Customer and/or ITS |
| OHS | Office of Healthy Schools |

1. Statement of Understanding
2. Throughout this document, references to this RFP will mean RFP document and all accompanying attachments exhibits and appendices.
3. Unless otherwise specified, throughout this document, references to the proposed solution will represent the collective services, system, or solution(s) being sought by the State.
4. Offerors should expect to find Exhibit F, Cost Information Submission form in the RFP, rather than in this Attachment A document.
5. Offerors should expect to find Exhibit D for the Reference forms in the RFP, rather than in this Attachment A document.
6. The State expects the Offeror to be capable of implementing a solution that will enable the State to fully manage and comply with the goals and requirements of the CMS. The State expects the Offeror to cure known deficiencies in the incumbent solution, enhance incumbent workflows, and automate manual processes.
7. Offerors must agree to provide best practices, industry-standard tools, and methodologies. The Offeror acknowledges that the State will not accept proprietary formats.
8. The Offeror will be responsible for implementing the proposed solution. The comprehensive solution proposed by the Offeror must address the general and functional requirements outlined in this RFP, including all applicable State and Federal requirements.
9. The solution must be compatible with current Microsoft products available through the MDE enterprise agreement. These include, but are not limited to, Microsoft Office 365 and SharePoint
10. The Offeror must propose a single release implementation designed to replace the incumbent solution with limited interruption to service/business operations. Any interruption to current operations must be conducted to prevent loss of service and must be approved by MDE.
11. The federal regulations governing State participation in the CMS are found in Title XIX of the Federal Social Security Act Section 1903 (a)(7) of the Act; 42 CFR 430.1 and 42. The Offeror must acknowledge these regulations, and the Offeror’s proposed solution must position the State to comply with any related regulations and requirements.
12. MDE acknowledges that the specifications within this RFP are not exhaustive. Rather, they reflect the known requirements that must be met by the proposed system. Offerors must specify here what additional components may be needed and are proposed to complete each configuration. Any costs associated with a complete system operation must be included in the Offeror’s proposed cost (Exhibit F, Cost Information Submission) or Offeror may face providing the additional components at not cost to the State.
13. Hosting Environment
14. Customer is seeking a cloud-hosted solution but will consider a Vendor-hosted solution. Offerors should indicate here where the proposed solution will be hosted.
15. The cloud-hosted environment must be capable of supporting the Random Moment Time Study (RMTS) application at maximum user capacity as well as maintaining the system’s database functions. Startup capacity is estimated to be up to 1,000 users logging in to the system. The solution must be scalable to accommodate additional users at no additional cost to the Customer.
16. For the Vendor hosted solution, the Offeror must meet the following minimum requirements.
17. Offerors must provide Managed Services including migrating any on-premise data.
18. Offeror must provide professional services such as monitoring, help desk support, security, etc.
19. Offeror must provide cloud hosting details and pricing in Exhibit F, Cost Information Submission.
20. Data Ownership: MDE shall own all right, title and interest in all data used by, resulting from, and collected using the services provided. The Offeror shall not access MDE User accounts, or MDE Data, except (i) in the course of data center operation related to this solution; (ii) response to service or technical issues; (iii) as required by the express terms of this service; or (iv) at MDE’s written request.
21. Data Protection: Protection of personal privacy and sensitive data shall be an integral part of the business activities of the Offeror to ensure that there is no inappropriate or unauthorized use of MDE information at any time. To this end, the Offeror shall safeguard the confidentiality, integrity, and availability of MDE information and comply with the following conditions:
22. All information obtained by the Offeror under this contract shall become and remain property of MDE.
23. At no time shall any data or processes which either belong to or are intended for the use of MDE or its officers, agents, or employees be copied, disclosed, or retained by the Offeror or any party related to the Offeror for subsequent use in any transaction that does not include MDE.
24. Data Location: The Offeror shall not store or transfer MDE data outside of the United States. This includes backup data and Disaster Recovery (DR) locations. The Offeror will permit its personnel and contractors to access MDE data remotely only as required to provide technical support.
25. Encryption:
26. The Offeror shall encrypt all non-public data in transit regardless of the transit mechanism using MDE approved encryption methodologies and standards which are NIST 800 data in transit encryption standards.
27. The Offeror must submit encryption methodologies in writing annually for MDE approval.
28. For engagements where the Offeror stores non-public data, the data shall be encrypted at rest. The key location and other key management details will be discussed and negotiated by both parties. Where encryption of data at rest is not possible, the Offeror must describe existing security measures that provide a similar level of protection. Additionally, when the Offeror cannot offer encryption at rest, it must maintain, for the duration of the contract, cyber security liability insurance coverage for any loss resulting from a data breach. The policy shall comply with the following requirements:
    * + 1. The policy shall be issued by an insurance company acceptable to MDE and valid for the entire term of the contract, inclusive of any term extension(s).
        2. The Offeror and MDE shall reach agreement on the level of liability insurance coverage required.
        3. The policy shall include, but not be limited to, coverage for liabilities arising out of premises, operations, independent contractors, products, completed operations, and liability assumed under an insured contract.
        4. At a minimum, the policy shall include third party coverage for credit monitoring. notification costs to data breach victims; and regulatory penalties and fines.
        5. The policy shall apply separately to each insured against whom claim is made or suit is brought subject to the Offeror’s limit of liability.
        6. The policy shall include a provision requiring that the policy cannot be cancelled without thirty (30) days written notice.
        7. The Offeror shall be responsible for any deductible or self-insured retention contained in the insurance policy.
        8. The coverage under the policy shall be primary and not in excess to any other insurance carried by the Offeror.
        9. In the event the Offeror fails to always keep in effect the insurance coverage required by this provision, MDE may, in addition to any other remedies it may have, terminate the contract upon the occurrence of such event, subject to the provisions of the contract.
29. Breach Notification and Recovery: Unauthorized access or disclosure of non-public data is a security breach. The Offeror will provide immediate notification, and all communication shall be coordinated with MDE. When the Offeror or their sub-contractors are liable for the loss, the Offeror shall bear all costs associated with the investigation, response and recovery from the breach including but not limited to credit monitoring services with a term of at least three (3) years, mailing costs, Website, and toll-free telephone call center services. MDE shall not agree to any limitation on liability that relieves a Offeror from its own negligence or to the extent that it creates an obligation on the part of MDE to hold a Offeror harmless. All breach and recovery measures shall be in compliance with MDE policy.
30. Notification of Legal Requests: The Offeror shall contact MDE upon receipt of any electronic discovery, litigation holds, discovery searches, and expert testimonies related to, or which in any way might reasonably require access to the data of MDE. The Offeror shall not respond to subpoenas, service of process, and other legal requests related to MDE without first notifying MDE unless prohibited by law from providing such notice.
31. Termination and Suspension of Service: In the event of termination of the contract, the Offeror shall implement an orderly return of MDE data in CSV or XML or another mutually agreeable format. The Offeror shall guarantee the subsequent secure disposal of MDE data.
32. Suspension of services: During any period of suspension of this Agreement, for whatever reason, the Offeror shall not take any action to intentionally erase any MDE data.
33. Termination of any services or agreement in entirety: In the event of termination of any services or of the agreement in its entirety, the Offeror shall not take any action to intentionally erase any MDE data for a period of 90 days after the effective date of the termination. After such 90-day period, the Offeror shall have no obligation to maintain or provide any MDE data and shall thereafter, unless legally prohibited, dispose of all MDE data in its systems or otherwise in its possession or under its control as specified in section 33(d) below. Within this 90-day timeframe, Offeror will continue to secure and back up MDE data covered under the contract.
34. Post-Termination Assistance: MDE shall be entitled to any post-termination assistance generally made available with respect to the Services unless a unique data retrieval arrangement has been established as part of the Service Level Agreement Level 6 in Table 3: SLA Matrix.
35. Secure Data Disposal: When requested by MDE, the provider shall destroy all requested data in all its forms, for example: disk, CD/DVD, backup tape, and paper. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST) approved methods. Certificates of destruction shall be provided to MDE.
36. Background Checks: The Offeror warrants that it will not utilize any staff members, including sub-contractors, to fulfill the obligations of the contract who have been convicted of any crime of dishonesty. The Offeror shall promote and maintain an awareness of the importance of securing MDE's information among the Offeror's employees and agents.
37. Security Logs and Reports: The Offeror shall allow MDE access to system security logs that affect this engagement, its data, and/or processes. This includes the ability to request a report of the activities that a specific user or administrator accessed over a specified period as well as the ability for an agency customer to request reports of activities of a specific user associated with that agency. These mechanisms should be defined up front and be available for the entire length of the agreement with the Offeror.
38. Contract Audit: The Offeror shall allow MDE to audit conformance including contract terms, system security as appropriate. MDE may perform this audit or contract with a third party at its discretion at MDE’s expense.
39. Sub-contractor Disclosure: The Offeror shall identify all its strategic business partners related to services provided under this contract, including but not limited to, all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the Offeror, who will be involved in any application development and/or operations.
40. Sub-contractor Compliance: The Offeror must ensure that any agent, including a Offeror or subcontractor, to whom the Offeror provides access agrees to the same restrictions and conditions that apply through this Agreement.
41. Processes and Procedures: The Offeror shall disclose its non-proprietary security processes and technical limitations to MDE so that MDE can determine if and how adequate protection and flexibility can be attained between MDE and the Offeror. For example: virus checking and port sniffing — MDE and the Offeror shall understand each other’s roles and responsibilities.
42. Offeror Qualifications
43. The Offeror must provide an introduction and general description of its company's background
44. Offerors must have provided the services requested in this RFP for at least five years. Offeror must state the number of years in business providing these services.
45. If Offeror has been providing these services for fewer than five years, they must include other States as references.
46. If Offeror has been providing these services for fewer than five years, they must substantiate understanding of CMS guidelines.
47. The Offeror must specify the location of the organization's principal office and the number of executive and professional personnel employed at this office.
48. The Offeror must specify the organization's size in terms of the number of full-time employees, the number of contract personnel used at any one time, the number of offices and their locations, and its structure (for example, state, national, or international organization).
49. The Offeror must disclose any company restructurings, mergers, and acquisitions over the past three (3) years and any planned future restructurings or mergers.
50. Offeror Implementation Team
51. The Offeror must demonstrate that all team members have the necessary experience for the development, configuration, implementation, testing, user training, maintenance, and support of the services required by this RFP. At a minimum, the Offeror's response should include team member roles, functional responsibilities, and experience with projects similar in size and scope to the services required by this RFP.
52. Identify the key staff members who will be responsible for executing the various aspects of the project, including, but not limited to, the Project Manager, Development Team, Business Analyst(s), and Technical Architect(s).
53. For each participating key staff member, provide a summary of qualifications, years of experience, and length of employment with your company.
54. The Offeror must ensure that each team member assigned to this project can communicate clearly in English, both verbally and in written form.
55. Functional/Technical Requirements

A. Web Access

1. The solution must be web accessible to Customer staff and authorized external system users.
2. The solution must provide a user account management interface that allows for password complexity policies and self-service password reset. If OAuth 2.0 can be used for user authentication that would be preferred. User management activity should be logged and available for reporting. Logging should, at a minimum, provide details such as timestamp, user, IP, and action performed.
3. The solution must offer web portal access to credentialed users for customer-defined functions. The portal must be intuitive and easy to navigate.
4. The solution must be browser-neutral and compatible with the current and two preceding versions of common browsers, including Chrome, Microsoft Edge, Firefox, and Safari.
5. The solution must be accessible to all end-user equipment, such as desktops, laptops, tablets, and other devices.
6. Solution must not require any additional browser plugins like Java, etc.

B. Mobile Access

1. The solution must be accessible to iOS and Android mobile devices.
2. The solution must have offline functionality, which allows users to access, add, and edit data. When connectivity is restored, modifications must synchronize to the database.
3. The solution must include mobile applications for iOS and Android platforms for use in the field by Customer employees.
4. The solution must be compatible with Microsoft tablets, Android tablets, iOS devices, and related devices for the current and two immediately preceding versions.
5. The solution must incorporate mobile viewing for credentialed users.
6. The solution must accommodate system management functions on mobile platforms.
7. The solution must provide real-time data exchange with field devices having adequate access.
8. User Interface and User Experience
9. The proposed system should include at least distinct roles:
   1. MDE Specialist
   2. Medicaid Specialist
   3. SBAC District Coordinator
   4. SBAC Business Manager
10. MDE Specialist role must:
    1. Have the ability to set up future time studies.
    2. Resend emails for time studies or training invitations.
    3. Add Coordinator and Business Manager roles and add security information.
    4. Update participant information.
    5. Accept or reject moments.
11. The system must code moments (responses) following Activity Codes Description and Examples on pages 46-53 of the Mississippi School-Based Administrative Claiming Guide, included as Attachment B to the RFP.
12. System must flag moments with errors or if clarification is needed.
13. System will flag moments that need to be reviewed and centrally coded.
14. System must allow moments to be re-coded.
15. Medicaid Specialist role must:
    1. Be able to perform audit functions programmatically.
    2. Utilize ad hoc or preexisting reports that help ensure compliance based on federal and state guidelines.
16. SBAC Coordinator role must:
    1. Be able to edit and add Participants so they can receive invitations to complete training and complete surveys once they have completed training.
    2. Resend emails for training invitations.
    3. View Random Moment Surveys and see the percentage of surveys completed in real time.
    4. Utilize ad hoc or canned reports that will help manage school district profile.
17. Business Manager Role must:
    1. Be able to input all cost information into the system and submit quarterly invoices.
    2. Utilize ad hoc or preexisting reports for compliance.
18. Functional/Technical
19. The proposed solution must obtain staff pools and participant rosters.
20. The proposed solution must gather time study specifications such as workday hours and holidays.
21. The proposed solution must ensure response rates meet the expected amount.
22. The proposed solution must perform quality control on excess non-reimbursable responses by workers.
23. The proposed solution must contain ad hoc reports requested by agency staff.
24. The proposed solution must summarize results, including any modifications such as reallocating general administration and similar codes.
25. The proposed solution must create invoices based on time study results.
26. The proposed solution must calculate statewide quarterly claims per school district as indicated in the “Mississippi School-Based Administrative Claiming Guide (2010)”
27. The proposed solution must allow for secure logins with individual credentials.
28. The proposed solution must support the creation of MDE Specialists, Medicaid Specialists, SBAC Coordinator, SBAC Business Manager and participants and system permission and/or privileges based on workflow.
29. The proposed solution must have a unique dashboard for each role or can be customized to support each role.
30. The proposed solution should be able to email and track users’ completion of tasks and deadlines.
31. The proposed solution should be able to track error messages in transaction logs for administrators to review.
32. The proposed solution must include a training module with the following functionality:
    1. Training module must include what the program is and how to complete the surveys.
    2. When new participants are added to the employee roster, within 24 hours, they will receive an email notification with a link to training.
    3. Training module must take into consideration that end users may be accustomed to the previous rules, regulations, and terminology.
    4. A video or PowerPoint training with a quiz at the end.
    5. Participants who pass the quiz at the end of the training will be eligible and notified to participate in future time studies.
    6. Participants who fail the quiz at the end of the training will be required to retake the quiz.
33. The proposed solution will include Random Moment Time Study’s (RMTS).
    1. RMTS must be accessible by MDE Specialists and Medicaid Specialists.
    2. When an RMTS is created, Coordinators can view who has been assigned, their school location, the date, and if it has been completed.
    3. The MDE Specialist, Medicaid Specialist, Coordinator, and Business Manager will be able to see the percentage of surveys completed in real-time.
34. The included RMTS application will select random participants from a pool of eligible participants.
35. The RMTS application must contain a test bank of possible job duties for each approved job title.
36. The RMTS application must email selected participants a link to their time study.
37. In order to be eligible, Participants must:
    1. Have successfully completed training.
    2. Verified their email address.
    3. Verified their job title and notify SBAC Coordinator if it needs to be changed.
38. Nurse Database application proposed system should allow two distinct roles:
    1. MDE Specialist
    2. School Nurse
39. In the Nurse Database System, the MDE Specialist role must:
40. Be able to create school nurse profiles for school district/clinic/school information.
41. Perform security administration such as password resets, and reassignment based on demographic information of the school district.
42. Create a global survey/questionnaire that will be used by all school nurses and add questions as necessary and create them as necessary.
43. In the Nurse Database System, the School Nurse must:
44. Be able to add number of times a particular service was encountered daily, weekly or monthly.
45. Be able to update their profile information (change password and license information).
46. Open or close survey period in order to add or remove information if necessary.
47. The Nurse Database System must be a questionnaire/survey type application that will allow school nurses to:
48. Key information based on a series of questions related to services that are performed within the school district setting (daily, weekly, and monthly).
49. Have information broken down by school district/school/clinic.
50. Single sign on application that has security permissions.
51. The Nurse Database System must be easy and intuitive for users.
52. Workflow
53. The solution must accommodate configurable workflows and business rules that are common to best practice solutions, whether they are specified by this RFP.
54. Solution business rules and workflows must allow multiple related triggers.
55. The solution must provide configurable triggers that initiate events and/or data-driven workflow actions that result in automatic updates to targeted processes.
56. The solution must provide configurable time standards that trigger and route workflows based on multiple variables as defined by the Customer.
57. The solution must allow authorized users to redirect workflows in response to circumstances that require temporary or permanent changes.
58. The solution must automatically calculate workflow/task deadlines as determined by the Customer; this feature must be configurable.
59. Workflow routing must accommodate, track, and report on due dates as defined by the Customer.
60. The solution must simultaneously distribute tasks to relevant parties.
61. The solution must display workflows in simple, graphic formats easily understood by system users.
62. Workflow graphics must indicate the status of a work item in the workflow.
63. The solution must provide the ability to create and modify workflows using built-in administrative tools.
64. Customer prefers drag-and-drop tools to configure workflows through a graphic user interface.
65. Authorized Customer staff must be able to reassign and override workflow tasks as necessary to manage workloads, staffing, and processes.
66. Reports and Dashboards
67. The solution must offer pre-designed, standard reports related to best practices, whether they are specified by this RFP.
68. **MANDATORY**: The solution must include a monthly usage report which shows how many surveys have been completed and how many have been assigned, either run through the solution or sent to the State by the Offeror. Offeror must provide samples of a report with their proposal response.
69. At a minimum, reports must include (samples of the reports are encouraged):
    1. Total Pool List
    2. Control List
    3. Trained Roster by District and Date
    4. Invoice Preliminary Report and Final Report
    5. Invoice Preliminary Detail Report and Final Report
    6. Invoice Preliminary Control Sheet and Final Report
    7. District Roster with Percentage of Trained Report
    8. Pass Responses
    9. RMS List Export
    10. Funds Certification Report
    11. RMS List by Quarter Report
    12. No Longer Employed Report
    13. District Closed Days Excel Export Report
70. The solution should include reports that show MDE Specialist, Medicaid Specialist, SBAC Coordinator, and SBAC Business Manager state level data such as:
    1. Employ visualization of data where appropriate.
    2. The number of users that replied per district vs the total number of participants selected for the random moment.
    3. Invoice amounts per quarter and decrease and/or increase based on prior quarters.
71. The solution must accommodate the creation and modification of standard reporting templates defined by the Customer.
72. The solution must accommodate user-defined reporting to create custom reports from all data elements for which the Customer requires tracking and reporting.
73. The user-defined reporting tool must be intuitive and easy for the user to comprehend.
74. The solution must provide the ability to save user-generated reports under user profiles.
75. The solution must allow authorized Customer staff to create their reports using an interface that does not require specialized knowledge of a third-party tool such as Crystal Reports.
76. The solution must allow Customer Staff to create and save customized reports and queries.
77. The solution must provide ad hoc reports of all users with system access, including the level of access and the date/time of last access.
78. The solution must be capable of exporting reports into file formats, including PDF, MS Excel, and MS Word.
79. The solution must be able to distribute reports through the workflow as email attachments.
80. Solution must provide a print view for the reports.
81. Solution must allow reports to be filtered from each dashboard by:
    1. Fiscal year
    2. Quarter
    3. Multiple years
    4. Months
82. The solution must provide dashboards that can be configured according to individual user’' roles and preferences of individual roles.
83. The solution must provide configurable dashboards for users to manage open tasks.
84. The solution must provide dashboard views that provide pertinent information related to workloads and tasks to assist in visualizing and prioritizing work.
85. The solution must automatically generate reports on a configurable schedule and distribute them to selected users as determined by the Customer.
86. The Nurse Database system must allow the MDE Specialist to create customized reports or allowed to export data from system.
87. The Nurse Database System must allow the School Nurse to print out reports that shows a cumulative total of how they answered their questions.
88. The Nurse Database system must allow for ad hoc or customized reporting to be done by:
    1. The end user.
    2. OHS staff.
89. The Nurse Database System must include a separate simple dashboard.
90. Notifications and Alerts
91. The solution must auto-generate emails or notifications based on conditions and thresholds set by the Customer.
92. The solution must provide email and correspondence templates for notification purposes.
93. The solution must provide task management functions that issue alerts for pending, due, or past-due tasks. This function should interface with the dashboard function to give users a visual representation of their tasks' status.
94. Task logs must reveal daily assigned tasks, task details, due dates, task status, and all other details pertinent to task management.
95. Search Function
96. The solution must offer best practice, full-featured, configurable data search functions that can be scheduled to run automatically and because of an individual request from an authorized user.
97. The solution must allow users to search by any indexable attribute required by the Customer.
98. The solution must be able to produce search results that represent the search term and subtle variations of it.
99. Searches must be exportable or downloadable to common file formats such as Excel, PDF, XML, and CSV.
100. Users must be able to save frequently used searches for repeated use.
101. Users must be able to search for upcoming events, deadlines, or other quantifiable parameters determined by the Customer.
102. The solution must provide global search functionality. At a minimum, this function should allow a user to search for any data or combination of data in the system. The results should be presented in a prioritized structure determined by the relevance to the search criteria. All connected or relatable data based on the search criteria should be presented within the prioritized results.
103. Audit Function
104. For tracking and audit purposes, the solution must assign unique identifiers to all users.
105. The solution must timestamp all actions taken by users and reflect the activity in the audit trail.
106. The solution must maintain an audit trail of data changes, including but not limited to previous and new values, change dates, and the identity of the person making the change.
107. Audit trails must be accessible in real-time by authorized Customer staff.
108. The solution must also be able to produce an audit trail of each user's historical security access changes.
109. The base solution must offer common audit trail functions inherent to best practice SBAC solutions and must, at a minimum, include:
110. Ability to audit based on activity type (view, modify);
111. Ability to set audit requirements based on data type or service type;
112. Ability to set audit retention schedule based on data type or service type;
113. Ability to audit user activity, including but not limited to logins, logouts, and changes within a record;
114. Ability to restrict access to auditing data;
115. UI for query/search and reporting of audit data; and
116. The ability for users to customize audit reports.
117. Archival
118. Per the Customer’s retention schedule requirements, the solution must retain, in a non-proprietary format, a complete repository of all records, documents, and transactions for purposes of audit compliance based on the federal and state guidelines, or as specified by Customer.
119. Authorized Customer users must have access to all related archived records, documents, and transactions for a period of seven years.
120. Administrative Management
121. The base solution must offer administrative management features and functionality common to all best practice based on the approved SBAC plan solutions, whether specified by this RFP/Attachment A.
122. The proposed solution must allow for multiple individuals to be assigned to an Administrator role.
123. The proposed solution must allow users in an administrator role to assume another user’s role to what they would see and assist with troubleshooting.
124. The proposed solution must provide configurable, role-based administrative tools and controls.
125. The solution must allow authorized users to set security and permissions by user or user group, including customized access permissions.
126. The solution must be highly configurable and, at a minimum, allow authorized users to generate, modify, deactivate, and delete user accounts, as well as reset passwords.
127. The proposed solution must allow Administrator users to add or modify participant information for each school district.
128. Solution must be highly configurable and at a minimum, allow authorized users to add or edit school districts, schools, quarters, etc.
129. The solution must be highly configurable and, at minimum, allow authorized users to configure business rules, data elements, screens, workflows, triggers, navigation, and dashboards.
130. The proposed solution must allow for the use of multiple email templates.
131. The proposed solution must allow for email tracking. Tracking must include:
     1. Who receives emails or moments.
     2. What was received.
     3. Who completed moments.
132. The proposed solution must allow for emails to be unsent.
133. The proposed solution must allow for emails and moments to be scheduled ahead of time:
     1. Configure moments.
     2. Set global and district calendar dates for moments and holidays and specify valid and invalid dates.
     3. Add calendar dates for holidays before surveys are created.
134. The proposed solution must accommodate common administrative functions such as creating and maintaining user accounts, backing up and restoring files, exporting files, generating reports, etc.
135. Financial Management
136. Information should be based on SBAC plan and/or best practice according to federal and state guidelines.
137. Calendar Function
138. The solution must offer full-featured calendar functions that are common to all best practices the SBAC plan and/or best practice according to federal and state guidelines.
139. At a minimum, the solution must offer calendar functions as described below.
140. The ability to be uploaded based on specific data elements.
141. The ability to choose appropriate dates per quarter and for error detection to reduce non-compliance.
142. System/Solution Design

A. Data Management

1. Offeror shall not store or transfer State data outside of the United States. This includes backup data and disaster recovery locations. The Offeror will permit its personnel and contractors to access State data remotely only as required to provide technical support.
2. Offeror agrees that the State shall own all rights, titles, and interests in all data used by, resulting from, and collected using the services provided. The Offeror shall not access State user accounts or State Data, except during data center operations related to this solution, in response to service or technical issues as required by the express terms of this service or at the State’s written request.
3. Offeror agrees to maintain and archive State data in non-proprietary formats to facilitate any future transition from the hosted solution to another solution.
4. Data Migration
5. Offeror must successfully migrate all existing Customer data, housed in an on-premises SQL database, to the proposed solution. If necessary, Offeror is responsible for data conversion for the migration.
6. Offeror must acknowledge and agree that the Customer is the sole owner of all database content migrated from the current solution to the proposed solution and any future database content created within the awarded Offeror solution, with exclusive rights to use the database content without restriction.
7. If necessary, Offeror must agree that such migrated and future created database content will be accessible in a non-proprietary format acceptable to the Customer.
8. The solution must accommodate all document formats requiring migration with existing records. Document formats currently in use include all Microsoft Office formats, .pdf, and all photo formats.
9. All migrated historical data must be searchable and reportable.
10. If conversion and migration costs are not included in the solution's base quote, the Offeror must present them as separate line items in Exhibit F , Cost Information Submission. More details regarding data migration are listed in the Implementation Requirements section below.
11. Backup Services
12. The Offeror must be able to configure, schedule, and manage all data backups including, but not limited to, files, folders, images, system state, databases, and enterprise applications.
13. The Offeror must maintain backup system security and application updates.
14. The Offeror must provide cloud backup options.
15. The Offeror must agree that the proposed solution will be backed up (data and system configurations) daily for continuity of operations considerations.
16. The Offeror must agree that the proposed solution will permit system administrators to selectively create full and incremental backups of all files without impacting the system's functionality.
17. The Offeror must encrypt all backup files and data and manage encryption keys. At a minimum, the backup options must encompass a strategy of daily incremental and weekly full backups. All cloud instances must include options for snapshots and backups of snapshots.
18. The encrypted backup should be moved to another geographical cloud region. Regardless of the backup method, weekly full backups must include system State information. The customer retention requirement for all backups is 52 weeks. Backup retrieval must be started within two hours of notification from the Customer. The Offeror must monitor all disaster recovery instances, including replication and instance performances.
19. The solution must be capable of running backup reports weekly or in whatever sequence the Customer requires. For example, the report should reveal which jobs were completed, failed, restarted, etc.
20. The solution must be capable of on-demand and auto-run reporting for backup reporting.
21. The Offeror must be willing to provide backups on demand related to development, database changes, or emergencies.
22. Business Continuity/Disaster Recovery
23. If the Offeror’s host site experiences unsafe or inoperable conditions, the Offeror must be prepared to resume normal Customer operations within two business days of becoming compromised. So that the Customer can assess the Offeror’s ability to meet this requirement, the Offeror must submit, with its proposal, a preliminary Continuity of Operations Plan (COOP). COOP services include but are not limited to providing cloud computing, system data, and documentation to ensure essential services in the event of a disaster declaration. Essential services are defined as those functions that enable the Offeror to provide normal Customer operations under any circumstances which are Monday – Friday 8:00am – 5:00pm Central Standard Time.
24. At a minimum, the Preliminary COOP must:
25. Outline a decision process for determining appropriate actions in implementing COOP plans and procedures to resume essential operations within two business days of failure.
26. Describe procedures to restore system functionality and to protect the integrity of system data and other assets.
27. Describe plans to mitigate disruptions to operations and
28. Outline plans for a timely and orderly recovery from an emergency and to resume full service to users.
29. Upon implementation, the Customer and the awarded Offeror will update the COOP to:
30. Revise plans and procedures as appropriate.
31. Identify essential functions.
32. Identify and describe alternate facilities.
33. Identify vital records and databases.
34. Document testing, training, and monthly exercises and drills.
35. Establish a roster of fully equipped and trained State personnel with the authority to perform essential functions and activities and
36. Establish reliable processes and procedures to acquire resources necessary to resume essential operations and functions within two days of the disaster declaration.
37. In the event of a declared disaster, the Customer expects the Offeror to be completely responsible for the restoration of essential operations.
38. The Offeror will be expected to invoke the appropriate disaster recovery plan within four hours of the disaster declaration and the disruption of normal operations.
39. Customers must be able to log on to the failover system at the disaster recovery site at 100% operational capacity within two business days of the declaration of disaster.
40. In the event of a disaster declaration, the Offeror must maintain regular and consistent communications with the Customer, keeping all relevant managers and responders informed and updated on efforts to restore normal operations.
41. Offeror must agree that the proposed solution will maintain synchrony between the primary Customer site and the failover site to ensure that every transaction successfully enrolled in the operational site is still available in case of a switchover to the alternate site.
42. Implementation Requirements
43. Offeror Acknowledgement
44. This section outlines the Customer minimum expectations of the awarded Offeror for implementing the selected solution. Implementation deliverables will reveal the Offeror’s expertise in project management, proposed solution process management, improvement, data migration, acceptance testing, etc. The Customer expects the proposed preliminary implementation plans to be refined by the awarded Offeror and Customer project managers during implementation.
45. Upon award, the Customer intends for the requirements outlined in this section and the responding Offeror’s proposal, including any subsequent, agreed-upon provisions and revisions, to act as the Implementation Statement of Work.
46. The Offeror must acknowledge that he has read and understood the intent of this section, Implementation Requirements—Statement of Work.
47. **MANDATORY**: Offeror must assist with updating the Mississippi School Based Administrative Claiming Guide to match the current federal standards.
48. Offeror must include references for whom these services have been performed in the last five (5) years.
49. General Scope
50. The Offeror must agree to implement the awarded solution to achieve the following minimum goals:
51. Replicate existing system as outlined in SBAC plan.
52. Enhance functional, technical, and administrative capabilities of the incumbent system.
53. Update/enhance incumbent workflows and automate incumbent manual processes.
54. Migrate the incumbent database content from the existing solution to the selected solution.
55. Maintain historical data integrity if the proposed solution changes current Customer data formats.
56. The Offeror must extensively test the proposed solution to identify and correct deficiencies in base capabilities, customizations, integrations, interfaces, migrations, and Customer processes. Such efforts must include but may not be limited to:
57. On-site Testing.
58. COOP Testing.
59. User Acceptance Testing; and
60. Final Acceptance Testing.
61. The Offeror will be responsible for any interface, integration, conversion, migration, or other issues that may arise during implementation.
62. The Offeror must train system users and provide complete system documentation and user documentation.
63. Compliance Standards
64. The Offeror must comply with all federal and state regulations relating to the School Based Administration program. The Current Mississippi School Based Administrative Guide must be updated to match current (2023) federal regulations as part of the implementation process. The current Mississippi Based Administrative Guide can be found at Attachment B.
65. Project Management Plan
66. Project Management Plan (PMP): The Customer desires to implement the proposed solution rapidly after contract execution. So that the Customer can assess the Offeror’s ability to successfully implement the proposed solution, the Offeror must submit a preliminary PMP. At a minimum, the PMP must address design and development, all implementation tasks, data conversion and migration, estimated hours per task, major project milestones, quality assurance checkpoints, testing, and end-user training. The preliminary PMP must be submitted with the Offeror’s proposal.
67. Offeror’s PMP must include a preliminary Integrated Master Schedule (IMS). The IMS must estimate the time necessary to complete all implementation phases from the point of contract execution through completion of go-live, final system acceptance, and user training.
68. The PMP, which will require Customer approval, must reveal plans for multiple environments, including design and development, user testing, production, end-user training, and help desk support. All customizations, integrations, and interfaces must be tested and validated in the user-testing environment.
69. The Offeror’s PMP must reflect industry best practice standards and must detail the Offeror’s plans for planning, monitoring, supervising, tracking, and controlling all project activities.
70. The Offeror’s PMP must describe the organizational structure of the implementation team, team member roles and responsibilities, resources, processes, and all other information necessary for the Customer to assess your ability to manage the proposed solution.
71. Upon award, the Offeror and Customer will jointly modify the proposed PMP and IMS as appropriate to meet implementation objectives. The Customer expects the Offeror to work with the Customer project manager to ensure effective project management during all implementation phases and until final acceptance.
72. Regarding this procurement, state all Offeror assumptions or constraints regarding the proposed solution, overall project plan, timeline, and project management.
73. Identify any potential risks, roadblocks, and challenges you have encountered in similar implementations that could negatively affect the timely and successful completion of the project. Recommend a high-level strategy to mitigate these risks.
74. A Offeror’s PMP must address interface, integration, conversion, migration, or other issues that may arise during implementation.
75. The Customer will have limited resources available to the awarded Offeror for implementation.
76. System Design Document
77. Before implementation, the awarded Offeror must submit a System Design Document (SDD) for review and State approval. The SDD must:
78. Include a conceptual model of the system architecture. This can be illustrated by flowcharts.
79. Include descriptions and illustrations of modules that handle specific system tasks.
80. Include descriptions and illustrations of components that provide a function or group of related functions.
81. Include descriptions and illustrations of interfaces that share boundaries across the components where the system exchanges related information.
82. Include descriptions and illustrations of data flow and the management of this information.
83. Include complete workflows for all operational user and administrative functions.
84. Include database scheme, listing all the tables, fields, and characteristics.
85. When the SDD document has been approved by the State, the Offeror may proceed with implementation.
86. So that the Customer can assess the Offeror’s ability to prepare an SDD, the Offeror must submit a preliminary SDD or a sample SDD from a prior project of similar size and scope. The Offeror may redact sample plans from prior implementations if necessary. The preliminary SDD must be submitted with the Offeror’s proposal.
87. Data Conversion and Migration
88. So that the Customer can assess the Offeror’s ability to migrate Customer legacy data to the proposed solution, the Offeror must submit a preliminary Data Migration Plan (DMP). Highlight any known risk factors and present risk mitigation plans. The preliminary Data Migration plan must be submitted with the Offeror’s proposal.
89. The Data Migration Plan must specifically show how the Offeror intends to accurately and completely migrate Customer data, including conversion if necessary. The Offeror agrees to work with the Customer to define and execute data cleanup efforts before conversion/migration.
90. The Offeror must be specific about the proposed methodology, tools, data, facilities, personnel, and other resources required for the migration. Regarding personal and other resources, be specific about whether the resources are supplied by the Offeror, Customer, or other. The Offeror should keep in mind that the Customer has limited available resources.
91. The incumbent database is a SQL 2019 database that resides on a Windows Server 2022 VM. The database is approximately 250-300 MB in size.
92. The Offeror must detail data migration testing plans to validate the successful migration from the incumbent system to the proposed solution.
93. The Offeror must work with the Customer project implementation team to update and modify the preliminary data migration plan as appropriate.
94. The Offeror must agree that final data migration and data migration testing plans are subject to approval by the Customer.
95. The Offeror must propose a set of system acceptance validations/tests that will demonstrate that the Offeror has complied with the Data Migration Plan. This set of system acceptance validations/tests, along with the Data Migration Plan, must be approved by the Customer before any data migration occurs.
96. Upon award, the Data Migration Plan will be amended to meet specific migration needs determined by the Offeror and Customer. During/following conversion completion, the Offeror/Customer must perform the acceptance tests in the Data Migration Plan. The Customer will review the acceptance plan results and provide an acceptance or rejection letter signed by the proper Customer authority to the Offeror. Only if the Offeror receives the acceptance letter will the conversion be considered complete and accepted.
97. Integrations and Interfaces
98. Solution must be able to migrate the existing database to eliminate having to manually recreate current and historical data elements in the awarded solution. The Offeror must convert and migrate as necessary to build the database with current and historical data at no additional cost. If this is not possible, an agreeable solution must be reached in order to maintain historical data.
99. Cost for integrations and interfaces should be provided at no additional cost to the State.
100. Offeror must convert all existing customer system data from the resident system to the awarded solution including but not limited to information needed to support compliance documentation needed for Medicaid claims for school districts. Supporting attachments must accompany converted records as appropriate.
101. Offeror must sign a confidentiality agreement with the State prior to access to data.
102. Offeror must present a detailed conversion plan prior to conversion process.
103. Offeror must identify any required fields not currently populated by the resident system and a method to supply the same to the awarded solution.
104. Offeror must provide verifiable, statical information, such as record counts to prove the successful conversion of legacy data.
105. Offeror must acknowledge and agree that MDE OHS is the sole owner of any and all database content migrated from the current solution to the proposed solution and any future database content created within the awarded Offeror solution, with exclusive rights to use the database content without restriction.
106. Offeror must agree that such migrated database content and future created database content will be maintained in a non-proprietary format that is acceptable to MDE OHS.
107. Solution must accommodate all document formats that will require migration with existing records. Document formats currently in use include, but are not limited to: All Microsoft Office formats, .pdf formats, and all photo, video, and audio formats.
108. If conversion and migration costs are not included in the base quote for the solution, Offeror must present such costs as separate line item.
109. User Acceptance Testing Plan
110. The Offeror agrees to conduct a User Acceptance Testing Plan to prove that the proposed solution fully meets the requirements of this RFP .
111. Offeror agrees that UAT procedures will include proving all end-to-end workflows and all necessary Customer interfaces.
112. The Offeror agrees that UAT will provide a full suite of reports generated during the UAT period to validate the reporting functions.
113. Offeror agrees that all customizations, integrations, and interfaces must be tested and validated in the user testing environment.
114. The Offeror must agree to regular status meetings with the Customer project management team to review progress on UAT.
115. The Offeror agrees to submit meeting agendas, presentation materials, and subsequent meeting minutes.
116. The Offeror must submit, with their proposal, a preliminary, comprehensive UAT plan (UATP) to demonstrate the Offeror’s ability to conduct user acceptance testing for the proposed solution.
117. Offeror’s UAT plan must incorporate the following minimum components:
118. UAT Test Procedures and Methodologies.
119. UAT Test Report; and
120. Training Materials.
121. Upon award, the Offeror agrees to finalize the preliminary UAT plan with input from the Customer project team.
122. Offeror agrees that the final UAT plan requires approval from Customer.
123. Offeror agrees that Customer expects to witness the execution of the UAT.
124. Offeror agrees that Customer retains the right to determine the success or failure of individual UAT tests.
125. Offerors must provide the facilities, equipment, and personnel to support the services identified in UAT.
126. The Offeror must agree to provide the equipment and personnel to identify and resolve discrepancies between the results of the legacy system(s) and the results of the delivered system(s).
127. The Offeror must agree to take corrective measures at no additional cost to the Customer when such discrepancies result in a failure of the Offeror-delivered system(s).
128. User Training and Documentation
129. The solution must provide thorough online tutorials/training geared toward the proposed solution users. The solution must track the progress of participants enrolled in training.
130. The Offeror must provide training documentation and keep it updated as appropriate. The web-accessible format is acceptable to the Customer.
131. For general training purposes, the Offeror must provide a mock system containing Customer data for hands-on training for internal and external users. Web-accessible format is acceptable to Customer.
132. Prior to go-live, Offeror must provide on-site training for three to five primary system administrators (SAs) in all facets including but not limited to oversight, reporting, tasks, workflows, security, archival and audit trail functions.
133. Prior to go-live, Offeror must agree to adequately train Customer staff users in how to successfully perform their respective tasks and workflows.
134. Offeror must agree to train Customer staff users and administrators in the effective use of the document management system.
135. Training costs should be included in the Offeror’s base offering in RFP, Exhibit F (Cost Information Submission). Training that is considered to be outside the base offering must be presented as a separate line item in the Cost Information Submission.
136. Change Management and Control
137. Offeror must agree that upon award, Offeror will describe, justify, and submit all proposed changes to the agreed upon project deliverables to Customer for approval. Such proposed changes include but are not limited to project scope, any and all implementation requirements, technical, functional, and configuration requirements, and/or all other agreed upon project deliverables.
138. The Project Manager must develop a Change Management Plan (CMP) for Customer which will be executed during implementation and followed throughout the lifecycle of the EHR project. At a minimum, the CMP must include the following components:
139. Readiness assessments;
140. Communication and communication planning;
141. Change management activities/events and related roadmaps;
142. Coaching and manager training for change management;
143. Developing and providing all facets of user training, including train the trainer;
144. Mitigation of change resistance to the awarded solution;
145. Data collection, feedback analysis, and corrective actions;
146. Celebrating and recognizing success; and
147. After-project review.
148. Offeror must agree to follow the State’s process for change control, which consists of the following minimum components:
149. Change Request Identification via Change Request Form - Documentation of change details such as type of change, benefits of change, resources, time and cost estimates, authorizations, etc. (Offeror);
150. Change Request Assessment (State);
151. Change Request Analysis (State/Offeror);
152. Change Request Approval (State);
153. Change Request Implementation (Offeror, overseen by State); and
154. Change Log – Project details such as project number, priorities, target date, status, etc. (Offeror).
155. System Documentation
156. Offeror must provide complete system documentation and keep it updated as appropriate. Web-accessible format is acceptable to Customer.
157. Final Acceptance Review
158. Offeror agrees that upon the successful completion of all implementation phases, including end user training, Customer will conduct a Final Acceptance Review (FAR) to determine whether or not Offeror has satisfied the terms and conditions of the awarded contract, which includes the requirements of this RFP, Attachment A.
159. Software Administration and Security
160. General
161. For hosted services, the School Based Administration design must be compliant with the State of Mississippi Enterprise Cloud and Offsite Hosting Security Policy. The State of Mississippi Enterprise Cloud and Offsite Hosting Security Policy is accessible via the ITS website at [www.its.ms.gov](http://www.its.ms.gov).
162. Solution must provide all software and system administration security features common to best practice based on MDE software security policies and management solutions, whether or not specified by this RFP.
163. Solution must provide controlled access to features and functions by configurable, role-based permissions as defined by Customer.
164. Solution must allow the system administrator to set rights for access to data by individual or group.
165. Solution must prevent unauthorized access to the system.
166. Solution must auto terminate sessions after a specified time of inactivity.
167. **MANDATORY:** Solution must accommodate two-factor authentication.
168. Solution must accommodate administrator user rights to any and all workflows and tasks as determined by Customer.
169. Authorized Customer staff must be able to restrict specific user groups from being able to view or print certain types of documentation.
170. Roles, security, and access rights must be easily configurable without Contractor assistance.
171. The proposed solution must adhere to all current, relevant security, and privacy standards.
172. The proposed solution must offer up-to-date, best practice identity management tools to govern user access, such as forced password changes, historical password checks, and the setting of temporary passwords, etc. User management activity must be logged and be available for reporting. Logging must, at a minimum, provide details such as timestamp, user, IP, and action performed
173. The Offeror shall describe how their proposed solution adheres to established security and privacy standards such as HIPAA, Federal Information Security Management Act (FISMA), Privacy Act, Federal Tax Information (FTI), and other Federal and State laws, regulations, and policies.
174. The Offeror must describe their established business and technical protocols to ensure that the transmission and storage of information remains encrypted while in transit and at rest.
175. At the State's request, the Offeror shall invoke a process for masking, sanitizing, scrambling, or de-sensitizing sensitive data (e.g., PHI/PII) when extracting data from the production environment for use in another environment for testing purposes.
176. Security Audit
177. The Offeror must complete Risk Assessments and Security Audit reports on an annual basis and when additions or changes to functionality affect the security framework and architecture, or when a new vulnerability is identified.
178. The Offeror must cooperate and assist the State in responding to all Federal and/or State audit and review requests. The Offeror must provide audit support including random sample generation, data extracts, and hard-copy documents, and shall provide any requested data or information.
179. The Offeror must make themselves available for third party auditors that ensure compliance with State and Federal security and privacy rules. The Offeror must provide a mitigation plan for all reported deficiencies. Major and critical deficiencies shall be corrected within established and agreed upon timelines.
180. Support and Maintenance

A. Customer Support

1. The Offeror must provide a continual, around the clock (24/7/365), manned network operating center (NOC) support and monitoring. This includes but is not limited to operating system support, network monitoring and health performance, network availability, and network security reporting. These services must be offered within the continental United States.
2. Offeror must provide a toll-free telephone number for Customer staff to call 24/7/365 and an always-accessible website for trouble reporting. All telephone customer support must originate in the Continental United States and all support staff must be able to communicate clearly in the English Language.
3. Offeror must ensure that whenever possible, all maintenance and updates be completed between the hours of 5:00 PM and 6:00 AM Central Standard Time.
4. Offeror must disclose instances where a third party or sub-contractor is being used for any portion of customer support services, including the intake of reported problems.
5. Offeror must keep the appropriate Customer management and technical support staff updated on the status of trouble resolution.
6. Offeror agrees to provide adequate training for the effective access and use of support services as requested by the State.
7. Offeror agrees to provide always-updated documentation of all support processes.
8. Offeror agrees that ongoing maintenance and support includes the correction of deficiencies.
9. Offeror agrees that deficiencies may be identified as a result of Offeror’s own monitoring or by the State. State discovered deficiencies will be reported to Offeror’s customer support for trouble resolution.
10. Issue Tracking
11. The Offeror must use an industry standard tracking system to thoroughly document issues and requests for Customer.
12. Describe how operational trouble issues are submitted, prioritized, tracked, and resolved.
13. Describe how software performance issues are submitted, prioritized, tracked, and resolved.
14. Describe how user support issues are requested, prioritized, tracked and resolved.
15. Detail your escalation procedures for responding to trouble tickets, software performance, and user support issues.
16. The Offeror must provide a customer portal for Customer to track help desk ticketing and incident resolution.
17. For issue tracking, solution must be capable of on demand as well as auto-run reporting.
18. The Offeror must provide a monthly issue tracking report as defined by Customer. For example, the report must detail and comment on any open tickets at month’s end, all issues opened and closed within the past month, and other details as required by Customer.
19. Service Availability and Restoration
20. Offeror agrees to include as unavailable time, any scheduled outages for preventive maintenance and planned upgrades where the Customer users do not have access to and the use of awarded services.
21. System Monitoring
22. Offeror agrees to provide monitoring services to cover all the services provided by the Offeror, including but not limited to:
23. Network connectivity (i.e., whether the network is up or down, and real-time bandwidth usage);
24. Full stack application monitoring;
25. Services running on the operating systems;
26. Performance indicator;
27. Network latency;
28. Utilization (e.g., memory, disk usage);
29. Trending (for minimum of one year);
30. Sharing of the monitored data with Customer through a portal;
31. High Availability—provider must have capabilities to detect failover to another region or availability zone in the event Customer workload and services failover; and
32. Offeror must provide detailed examples of how it has integrated alerts that are triggered by monitoring technologies into their support processes.
33. System Availability Requirements
34. Customer requires that system be available Monday through Friday from 6:00 am to 5:00 pm Central Standard Time.
35. Customer requires notifications of service outages or degraded performance. The Offeror must communicate notifications via a support ticket, email, telephone call, or by all three methods, depending upon the severity of the situation. Upon service restoration, the provider shall provide fault isolation and root-cause analysis findings in restoration notices to Customer points of contact.
36. Offeror must provide root-cause analysis notifications within two business days of the incident. The Offeror must use proven technology, processes, and procedures to escalate problems to Customer points of contact via a call tree-based solution, depending on the severity and type of issue.
37. The Offeror must provide a work effort estimate once a root-cause analysis is complete and be willing to expedite issues which rate “Critical” or “Severe” depending on the root-cause.
38. The Offeror shall follow the problem severity guidelines specified in Table 1 for assigning severity levels for incident creation

| ***Table 1 - Deficiency Priority Levels*** | | | |
| --- | --- | --- | --- |
| **Priority Level** | **Description of Deficiency** | **Notification Timeframe** | **Resolution Time** |
| **1**  **Critical** | System is down (unscheduled downtime) or is practically down (e.g., extremely slow response time) or does not function at all, as determined by State. There is no way to circumvent the problem; a significant number of State users, administrators, and participants. A production business system is inoperable. | One hour  from discovery | Eight consecutive hours from discovery |
| **2**  **Severe** | A component of the solution is not performing in accordance with the specifications (e.g., slow response time), creating significant State business impact, its core functionality is not available, or one of system requirements is not met, as determined by State. | Four hours from discovery | 24 hours  from discovery |
| **3**  **Moderate** | A component of the solution is not performing in accordance with the specifications; there are unexpected results, moderate or minor operational impact, as determined by State. | 24 hours from discovery | 14 days  from discovery |
| **4**  **Low** | As determined by the State, this is a low impact problem, that is not significant to operations or is related to education. Some examples are: general *how to* or informational solution software questions, understanding of reports, general *how to create reports,* or documentation requests. | 48 hours  from discovery | Resolve educational issues as soon as practicable by Offeror. Low impact software or operational issues to be resolved by next version release or six months, unless otherwise agreed to by State and Offeror. |

1. Remedies for Failure to Meet Service Levels
2. Offeror agrees that liquidated damages will accrue for unscheduled downtime, including Offeror’s failure to meet system availability requirements or response time requirements for curing deficiencies.
3. For purposes of assessing liquidated damages, response timeframes will be measured from the time the Offeror is properly notified until the State determines that the deficiency has been resolved.
4. All deliverables are subject to liquidated damages. The parties recognize the importance of timely completion of surveys for the Mississippi Department of Education, districts, schools, students, and parents of students. The parties agree that Offeror’s nonperformance will result in injury to MDE. Nonperformance is defined as Offeror’s failure to maintain service levels.
5. The parties agree that if nonperformance were to occur, it would be difficult to determine damages. Based on what the parties presently know, the parties agree that the amount of liquidated damages as set forth below are fair and reasonable and would not act as a penalty to the breaching party. MDE shall notify Offeror in writing of any claim for liquidated damages.
6. Parties agree to the following liquidated damages for Offeror’s nonperformance:
   1. Interrupted or slowed survey administration such as issues pertaining to outages and/or slowed responsiveness shall be assessed liquidated damages in an amount up to or equal to $500 per day not to exceed 7% total value of the contract for the fiscal year in which the nonperformance occurs.
   2. Test content during administration such as issues with item rendering, item versioning, item selection/ordering shall be assessed liquidated damages in an amount up to or equal to $500 per day not to exceed 5% total value of the contract for the fiscal year in which the nonperformance occurs.
   3. Test security such as unauthorized access and/or unauthorized exposure to assessment content shall be assessed liquidated damages in an amount up to or equal to 5% total value of the contract for the fiscal year in which the nonperformance occurs.
   4. Data privacy and/or security such as unauthorized access and/or unauthorized exposure of personal identifiable information of student, teacher, the MDE staff, or other individuals shall be assessed liquidated damages in an amount up to or equal to 5% total value of the contract for the fiscal year in which the nonperformance occurs.
   5. Unrecoverable data loss and/or corruption such as orphaned data, missing data and/or mis-linked data shall be assessed liquidated damages in an amount up to or equal to 7% total value of the contract for the fiscal year in which the nonperformance occurs.
   6. Score validity (after reports are released) such as inaccurate item scores, inaccurate scale scores, and/or inaccurate performance levels shall be assessed liquidated damages in an amount up to or equal to 7% total value of the contract for the fiscal year in which the nonperformance occurs.
7. Patching
8. The Offeror must provide patching capabilities for all Customer systems in the cloud. Patching must cover all Microsoft and non-Microsoft vulnerabilities.
9. The Offeror must manage deployment of new patches in Customer environment before production deployment and must be capable of excluding patches from normal patching based on requests from Customer. This may include service packs and other application-specific patches.
10. The Offeror must provide Customer with a list of patches to be applied before each patching event.
11. From time to time, Customer may request that specific patches be performed outside of the normal monthly patching cycle. The provider must be capable of support these out-of-cycle patch requests.
12. Software/Product Updates
13. Once available, Offeror must provide all software updates necessary to keep current with the proposed solution’s technology standards, industry standards, third party software upgrades, enhancements, updates, patches, and bug fixes, etc.
14. Such Software updates shall include but not be limited to enhancements, version releases, and other improvements and modifications to the core solution software, including application software.
15. Offeror agrees that maintenance services will also include maintaining compatibility of the solution software with any and all applicable contractor provided interfaces.
16. Offeror agrees that prior to installation of any third-party software or any update thereto, Offeror must ensure compatibility, promptly upon release, with the then current version of the software.
17. Offeror agrees to ensure compatibility with all required or critical updates to third party software, including without limitation, service and compatibility packs, security patches, and updates to operating systems.
18. Offeror agrees that third party application software incorporated by the Offeror is subject to the same maintenance and service obligations and requirements as the application software components that are owned or are proprietary to the Offeror.
19. Technology Refresh and Enhancements
20. Offeror agrees to conduct joint technology reviews with the State to guarantee that the software and system security are adequate for State purposes and are consistent with then-current technology used in similar systems.
21. Change Order Rate
22. After implementation and acceptance of the services procured by this RFP, Customer may require additional services, such as enhancements or other system related needs. Offer must include a fully loaded change order rate as a separate line in the Offeror’s Cost Information Submission, Exhibit F of this RFP
23. Deliverables
24. Offeror must agree to provide the deliverables described in Table 2 below. So that the State can evaluate Offeror capabilities, make preliminary deliverables as detailed as possible to show compliance with the specific RFP requirements. Post award and prior to implementation, Offeror and MDE will amend deliverables as appropriate. MDE approval is required for all deliverables prior to implementation.

| ***Table 2 - Deliverables*** |  |
| --- | --- |
| **Deliverables Title** | **Delivery Date** |
| **Hosting Requirements** | With proposal and with update – within 30 days after the Effective Date of the Agreement |
| **Integrated Master Schedule** | With proposal and with update at Project Management Reviews |
| **Test and Evaluation Master Plan** | With proposal and with update – within 30 days after the Effective Date of the Agreement. This Master Plan, which should include a discussion of SAT and UAT, should be submitted as a preliminary plan with the proposal. The Test and Evaluation Plan is an umbrella document covering all phases of system testing and evaluation and all forms of testing |
| **Migration Plan** | At System Design Review. The System Migration Plan and the Data Migration Plan are to be submitted as preliminary plans with Offeror’s proposal |
| **Test Reports** | Several sets, each corresponding to the outcomes of Factory Acceptance Test, System Acceptance Test and User Acceptance Test. For each increment, at Pre-Ship Review and Operational Readiness Review. |
| **Agenda** | Five (5) Business Days prior to a meeting |
| **Presentation Materials** | Draft – five (5) Business Days prior to a meeting, with Updates – at the meeting and final – as part of Minutes. |
| **Minutes** | Draft – two (2) Business Days after the meeting, with final – five (5) Business days after receipt of State Comments. |
| **User Manuals** | At each training session and for online reference |
| **Database Design Document** | Draft – five (5) Business Days prior to System Design Review, with updates – at the review, and Final as part of System Acceptance |
| **Interface Design Document** | Draft – five (5) Business Days prior to System Design Review, with updates – at the review, and Final as part of System Acceptance |
| **System Design Document** | Draft – five (5) Business Days prior to System Design Review, with updates – at the review, and final – as part of System Acceptance. |
| **Installation Plan** | For each delivery, at Product Test and Readiness Review or 12 weeks prior to installation, whichever is earlier, with updates – at Pre-Ship Review |
| **Training Plan** | At System Design Review with updates – at Pre-Ship Review |
| **Installation Drawings** | At System Design Review with updates – at Pre-Ship Review |
| **Training Materials** | For each delivery, at Product Test and Readiness Review or 12 weeks prior to installation, whichever is earlier, with updates – at Pre-Ship Review |
| **Technical Report** | As specified, or required, or requested by State. |
| **Test Procedures** | Draft – 30 working days prior to Product Test and Readiness Review and System Test and Readiness Review, with updates – at the review, and final – as part of User Acceptance Testing |
| **COOP Plan** | At System Design Review with revision – at Pre-Ship Review |
| **System Hardware** | Review prior to Operational readiness |
| **Software Licenses** | Review prior to Operational Readiness |
| **System Data** | Review prior to Operational Readiness |
| **Version Description Document** | At Pre-Ship Review with updates – at Operational Readiness Review and Final Acceptance Review. |
| **Installation Survey Report** | At completion of each site survey. |
| **Test Plan** | At System Design Review with revision – at Test Readiness Review |
| **Configuration Management**  **Plan** | Within 30 days after the Effective Date of the Agreement. |
| **Requirements Verification**  **and Traceability Matrix** | Draft – five (5) Business Days prior to System Design Review, with updates – at the review, and final – as part of User Acceptance Testing. |
| **System Performance Report** | Periodic logs of all transaction and System activity necessary to evaluate Agreement performance and to facilitate trend analysis, support system and other transactional analysis as specified in this RFP. |
| **Data and Property**  **Management Plan** | Offeror must develop, document and implement comprehensive procedures for the management of data, documentation and State property (equipment, hardware or software that belongs to State). |
| **Service Level Plan** | In accordance with the functional, technical, maintenance, and support requirements of this RFP, Offeror must develop a Service Level Plan (SLP) to govern Offeror’s performance after system acceptance. The SLP must meet the performance  Reporting requirements outlined in Offeror requirements. |