

Attachment A

to

RFP 4689

Mississippi Department of Health
(MSDH)
WIC Text Messaging

Technical Requirements

ITS Project No. 48935

TABLE OF CONTENTS

- I. General..... 1**
 - A. How to Respond to this Section..... 1
 - B. General Overview and Background..... 1
 - C. Statement of Understanding..... 2
 - D. Vendor Qualifications 2

- II. Functional/ Technical Requirements 2**
 - A. System Requirements/Capabilities 2
 - B. Administrative Management..... 4
 - C. Access 4
 - D. Reports and Dashboards..... 5
 - E. Archival 5
 - F. Audit Functions..... 5

- III. Support and Maintenance..... 6**
 - A. Customer Support 6
 - B. Issue Tracking..... 6
 - C. Service Level Agreements..... 6
 - D. Remedies for Failure to Meet Service Levels 8

- IV. Hosting Environment 9**
 - A. General 9
 - B. Business Continuity/Disaster Recovery 10
 - C. State of Mississippi Enterprise Cloud and Offsite Hosting Security Policy 10

- V. Implementation Requirements – Statement of Work 13**
 - A. Vendor Acknowledgement..... 13
 - B. Project Management Plan 14
 - C. Acceptance Test Plan..... 14
 - D. Training Requirements 15

- VI. Other 15**
 - A. Other Requirements..... 15

Attachment A

RFP No. 4689 – WIC Text Messaging

I. GENERAL

A. How to Respond to this Section

1. Beginning with Item 11 of this section, label and respond to each outline point in this section as it is labeled in the RFP.
2. The State is under the impression that Vendors have read and agree to all items in this RFP. Vendors should take exception to items in which they disagree.
3. The Vendor 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 Vendor receiving a lower score for that item, or, at the State’s sole discretion, being subject to disqualification.
4. “WILL COMPLY” indicates that the vendor can and will adhere to the requirement. This response specifies that a vendor or vendor’s proposed solution must comply with a specific item or must perform a certain task.
5. If the Vendor cannot respond with “WILL COMPLY”, then the Vendor must respond with “EXCEPTION”. (See Section V, for additional instructions regarding Vendor exceptions.)
6. Where an outline point asks a question or requests information, the Vendor must respond with the specific answer or information requested.
7. In addition to the above, Vendor must provide explicit details as to the manner and degree to which the proposal meets or exceeds each specification.

B. General Overview and Background

The WIC Program provides nutritious foods, nutrition education, and referrals to pregnant, breastfeeding, and postpartum women, infants, and children up to five years of age who are determined to be at nutritional risk and meet income guidelines. The program is designed to positively impact prenatal nutrition, infant birth weight, iron deficiency anemia, early childhood nutrition, and cognitive development. WIC must comply with Federal and State guidelines and reporting requirements. The WIC Program is funded by the United States Department of Agriculture (USDA), governed by Federal Regulations contained in the Federal Register 7CFR Part 246, and is generally administered by state governments. The Food and Nutrition Services (FNS) of the U.S. Department of Agriculture provides funds to the Mississippi State Department of Health for food benefits, nutrition services, and administration of the Program. Eligibility in the WIC Program is based upon four criteria: categorical eligibility, nutrition risk, income, and residency in a specific service area.

Mississippi provides WIC services to approximately 65,000 participants monthly. Clinic services which include health screenings, program eligibility determination, and issuance of WIC food instruments, nutrition education and referral occur through about 206 clinics statewide. Food delivery services for WIC participants are administered through approximately 294 WIC- authorized vendors, including grocery stores and pharmacies.

MSDH WIC Program would like to continue services with a company to deliver HIPAA compliant messages via telephone, text and/or email to WIC participants. The contractor shall provide MSDH with professional appointment reminder services. Services shall include, but are not limited to, the following: Automated messaging services that include

Attachment A

RFP No. 4689 – WIC Text Messaging

telephone, text messages, and or emails. Messaging shall include appointment reminders, no-show follow up, annual/recall notices, immunization notices, WIC pick-up notices, clinic closures/provider rescheduling notices for WIC participants. The contractor must have a two-way interactive feedback option such as confirm, cancel, repeat mechanism. Contractor must provide automated conversational texting services that include sent and received texts. Reports must be accessible.

C. Statement of Understanding

8. Throughout this document, references to this RFP will mean RFP No. 4689, including Attachment A to RFP 4689, and all accompanying exhibits and appendices.
9. 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.
10. ITS acknowledges that the specifications within this RFP are not exhaustive. Rather, they reflect the known requirements that must be met by the proposed system. Vendors must specify, here, what additional components may be needed and are proposed in order to complete each configuration.

D. Vendor Qualifications

11. Vendor must have proven experience in providing mass messaging systems for WIC programs.
12. Vendor must demonstrate ability to support multilingual communication and mobile access.
13. Vendor must provide a description of the organization to include the following:
 - a. Company background and history.
 - b. Examples of relevant projects, particularly in providing services for WIC programs
 - c. Video demo of features that doesn't exceed longer than 30 minutes
14. Vendor must have been in the business of providing such solutions for at least the past three years.
15. The Vendor must provide a list of current governmental clients and/or other public entities to demonstrate prior experience.
16. If the Vendor is a subsidiary, documentation for the parent company must also be provided.

II. FUNCTIONAL/ TECHNICAL REQUIREMENTS

A. System Requirements/Capabilities

17. **MANDATORY:** The solution must provide automated appointment reminders and missed appointment notifications.
18. **MANDATORY:** The solution must provide real time, 2-way conversational text messaging for appointment reminders, and ongoing direct participant engagement.
19. **MANDATORY:** The solution must provide closed clinic and emergency messages.

Attachment A

RFP No. 4689 – WIC Text Messaging

20. **MANDATORY:** The solution must support the capability to deliver targeted, real-time messaging to defined groups or sub-groups.
21. **MANDATORY:** The solution must provide text and email messages in English and Spanish. Other languages are optional.
22. **MANDATORY:** The solution must view real time text and voice responses from the web portal.
23. **MANDATORY:** The solution’s chat texting capabilities must not require an App for the participant.
24. **MANDATORY:** The solution’s chat texting capabilities must include useful features such as auto translate, clinic out-of-office auto responses, and chat templates.
25. **MANDATORY:** The solution must offer chat messages from current, local, and recognizable phone numbers that support sender identification.
26. **MANDATORY:** The solution must allow messages to be sent multiple times with settable rules. For example, a text message and voice message are sent days before the appointment, and if no response is received a follow-up text message is sent one (1) day before the appointment.
27. **MANDATORY:** The solution must provide multiple levels of access. Access allows Admins to have a high level of control, while also allowing autonomy for its users at the agency and clinic levels who can send messages and view results only to participants within their areas.
28. **MANDATORY:** The solution must be capable of creating its own messages or using our pre-defined scripts when needed.
29. **MANDATORY:** The solution must comply with HIPAA requirements due to the system transmitting and storing Protected Health Information (PHI).
30. **MANDATORY:** The proposed system must be able to communicate effectively with the following audiences:
 - a. WIC participants
 - b. WIC staff
31. **MANDATORY:** The system must provide support for the following types of communication:
 - a. One- Way Text Messaging
 - b. Emails
 - c. Telephone
 - d. Two-Way Messaging
32. **MANDATORY:** The solution must provide automated messaging services that include telephone, text messages, and/or emails.
 - a. Messaging shall include appointment reminders, no-show follow up, annual/recall notices, immunization notices, WIC pick-up notices, clinic closures/provider rescheduling notices for WIC participants.
 - b. Vendor must have a two-way interactive feedback option such as confirm, cancel, repeat mechanism.

Attachment A

RFP No. 4689 – WIC Text Messaging

- c. Vendor must provide automated conversational texting services that include sent and received texts.
 - d. Reports must be accessible to MSDH.
- 33. **MANDATORY:** The solution must support configurable consent management (opt-in/opt-out) and maintain records of consent.
 - 34. **MANDATORY:** The solution must include automated opt-out handling (e.g., STOP) and opt-in handling (e.g., START).
 - 35. **MANDATORY:** The solution must prevent sending messages to opted-out recipients unless re-consent is documented.
 - 36. **MANDATORY:** The solution must allow the State to increase or decrease message volume and/or user count.
 - 37. **MANDATORY:** The solution must be capable of sending and receiving a minimum of 30,200 outbound messages per month and 14,000 inbound SMS messages, phone calls, or emails per month.

B. Administrative Management

- 38. **MANDATORY:** The solution must provide configurable user notification creation and tracking capabilities.
- 39. **MANDATORY:** The solution must force consistent data entry parameters as determined by MSDH. For example, the solution should ensure consistent name and address formats including name suffixes, hyphens, common address abbreviations, etc.
- 40. **MANDATORY:** The solution must minimize redundant data entry and data manipulation. For example, solution must auto-populate fields with data from related fields where applicable.
- 41. **MANDATORY:** The solution must support password policies that meet State security standards (minimum length, complexity, expiration).
- 42. **MANDATORY:** Vendor must allow administrators to create, edit, suspend, and deactivate user accounts.
- 43. **MANDATORY:** The solution must accommodate the need for MSDH and Provider system administrators to perform necessary administrative functions including but not limited to creating and maintaining user accounts, backing up and restoring files, exporting files, and generating reports, etc.

C. Access

- 44. **MANDATORY:** The solution must support role-based access control (RBAC) for different user roles (e.g., Admin, Supervisor, Standard User, Read-only).
- 45. **MANDATORY:** The solution must support secure access to restricted functionality through a protected login in accordance with access privileges of that specific user.
- 46. **MANDATORY:** The solution must be configurable to accommodate various data types and user functions.
- 47. **MANDATORY:** The solution must support logging and reporting of system access by user, type, and/or agency.

Attachment A

RFP No. 4689 – WIC Text Messaging

48. **MANDATORY:** The solution must provide real-time data exchange with mobile devices for authorized users having adequate access.

D. Reports and Dashboards

49. **MANDATORY:** Solution must provide dashboards showing message delivery status (sent, delivered, failed, undeliverable).
50. **MANDATORY:** Solution must provide reporting on inbound and outbound message volume by date range, program, and user.
51. **MANDATORY:** Solution must track and report opt-in and opt-out activity.
52. **MANDATORY:** Solution must allow filtering and searching of message history by phone number, first name, last name, date, keyword, and delivery status.
53. **MANDATORY:** Solution must provide analytics for campaign performance (i.e. response rates, engagement rates, etc.).
54. **MANDATORY:** The solution must accommodate the creation and modification of standard reporting templates for each using and/or authorizing entity as defined by MSDH.
55. **MANDATORY:** The solution must accommodate user-defined reporting for the purpose of creating custom reports from any and all data elements for which MSDH requires tracking and/or reporting.
56. **MANDATORY:** User defined reporting tool must be intuitive and easy for the user to comprehend.
57. **MANDATORY:** The solution must provide configurable reporting of all system activity, as required by MSDH.
58. **MANDATORY:** The solution must provide the ability to save user-generated reports under user profiles.
59. **MANDATORY:** The solution must provide configurable dashboards on performance measures and system activity, such as active users, etc.

E. Archival

60. **MANDATORY:** Solution must retain message history for a minimum of three (3) years in accordance with Agency and Federal retention policies.
61. **MANDATORY:** Authorized MSDH users must have access to all archived records, documents, and transactions.

F. Audit Functions

62. **MANDATORY:** The solution must assign unique identifiers to system transactions to facilitate MSDH auditing functions.
63. **MANDATORY:** Vendor must provide access to message logs for auditing and compliance review.
64. **MANDATORY:** For tracking and audit purposes, solution must assign unique identifiers to all authorized users.
65. **MANDATORY:** The solution must provide audit trails for user activity (logins, message sends, contact edits, exports).

Attachment A

RFP No. 4689 – WIC Text Messaging

- a. Actions taken by all users should be time-stamped and reflected in the audit trail.
- 66. **MANDATORY:** The solution must maintain audit trails of data changes including but not limited to previous and new values, change dates, and the identity of the person making the change.
- 67. **MANDATORY:** Audit trails must be accessible in real time by authorized MSDH staff.
- 68. **MANDATORY:** The solution must also be able to produce an audit trail of the historical security access changes for each user.
- 69. **MANDATORY:** Audit trails must be customizable and exportable in common report formats.
- 70. **MANDATORY:** Audit trails must be retained and accessible for the current month and the prior thirty-six months.

III. SUPPORT AND MAINTENANCE

A. Customer Support

- 71. The Vendor must provide MSDH with enhancements and updates to the proposed solution as they are made generally available.
- 72. The Vendor must identify and explain the process through which MSDH is notified when new functionality is provided, or other enhancements are made to the proposed solution.
- 73. The Vendor must provide help-desk support for MSDH staff and end users of the system to assist with log-in issues, accessing content, etc. Help-desk support should be available Monday to Friday, 8:00AM-5:00PM Central Standard Time (CST) at minimum. Help-desk support should include phone and email options at minimum
- 74. Vendor must provide a help-desk process with ticket tracking and escalation procedures.

B. Issue Tracking

- 75. The Vendor must use an industry standard tracking system to thoroughly document issues and requests for MSDH.
- 76. The Vendor must describe how operational trouble issues, software performance, and support issues are submitted, prioritized, tracked, and resolved.
- 77. The Vendor must detail escalation procedures for responding to trouble tickets, software performance, and user support issues.

C. Service Level Agreements

- 78. MSDH requires notifications of service outages or degraded performance. The Vendor shall 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 MSDH points of contact.

Attachment A

RFP No. 4689 – WIC Text Messaging

79. Vendor must provide root-cause analysis notifications within two (2) business days of the incident. The Vendor must have proven technology, processes, and procedures to escalate problems to MSDH points of contact via a call tree-based solution, depending on the severity and type of issue.
80. The Vendor 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.
81. The provider shall follow the problem severity guidelines specified in Table 1 for assigning severity levels for incident creation.
82. For the initial term and any extended terms of service, the Vendor must agree that, except as the result of a catastrophic event, Vendor will provide least 99.98% percent availability of all MSDH registration system services, to be measured monthly.

Table 1 – Service Level Agreement

Priority Level	Description of Deficiency	Response Required	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, including distributors and recipient agencies are affected. A production business system is inoperable.	Within one hour from intake	Eight consecutive hours from intake
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.	Within one hour from intake	Ten consecutive hours from intake
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.	Within one hour from intake	Seven days from intake
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 <i>how to</i> or informational solution software questions, understanding of reports, general <i>how to create</i>	Within one hour from intake	Low impact software or operational issues to be resolved by next version release unless otherwise agreed to by State and Vendor.

Attachment A

RFP No. 4689 – WIC Text Messaging

	reports, or documentation requests.		
--	-------------------------------------	--	--

D. Remedies for Failure to Meet Service Levels

83. Vendor agrees that service credits will accrue for unscheduled downtime, including Vendor's failure to meet system availability requirements or response time requirements for curing deficiencies.
84. For purposes of assessing service credits, response timeframes will be measured from the time the Vendor is properly notified until the State determines that the deficiency has been resolved.
85. For purposes of assessing service credits, Vendor agrees that credits will be measured in monthly cumulative hours/minutes for unresolved deficiencies and unscheduled downtime.
86. Vendor agrees that Priority Levels 1 and 2 response time deficiencies will be considered unscheduled downtime and will entitle the State to service credits in accordance with Table 2, Service Credit Assessments.
87. Without limiting any other rights and remedies available to State, Vendor agrees to issue service credits in accordance with the measures prescribed by Table 2, Service Credit Assessments.
88. Vendor agrees that service credits will be calculated separately for each applicable deficiency and will be assessed at the end of each month of system maintenance.
89. Vendor agrees that after thirty (30) days of continued, deficient response time, according to the SLA, the State will consider the conditions to be equal to unscheduled downtime and the service credits in Table 2 will go into full force and effect.
90. In the event of repeated violations of a single SLA measure or multiple failures across SLA measures over two consecutive months, the State reserves the right to renegotiate SLA measures.
91. Vendor agrees that service credits are not penalties and, when assessed, will be deducted from the State's payment due to the Vendor.
92. Vendor agrees to include as unavailable time, any scheduled outages for preventive maintenance and planned upgrades where the MSDH users do not have access to and the use of awarded services.

Table 2a – Service Credit Assessments for Unscheduled Downtime

Length of Continuous Unscheduled Downtime	Service Credits
1 to 4 hours	One day of Service Credits equal to 1/30th of Monthly Fees
4 to 48 hours	Two days of Service Credits equal to 1/15th of Monthly Fees
48 to 96 hours	Five days of Service Credits equal to 1/6th of Monthly Fees

Attachment A
RFP No. 4689 – WIC Text Messaging

Each additional block of 96 hours thereafter	Additional Five days of Service Credits equal to 1/6th of Monthly Fees
--	--

Table 2b – Service Credit Assessments Per Incident for Timeframes Defined in Table 1

Priority Level	Service Credit for Failure to Meet Response Requirement	Service Credit for Failure to Provide Action Plan/Follow Up	Service Credit for Failure to Meet Resolution Requirement
Severity 1 – Critical Respond: 1 – 2 hours Action Plan: 4 – 8 hours Resolve: 12 hours	\$1,500.00	\$1,500.00	\$3,000.00
Severity 2 – Severe Respond: 2 – 3 hours Action Plan: 8 – 12 hours Resolve: 24 hours	\$1,000.00	\$1,000.00	\$2,000.00
Severity 3 – Moderate Respond: 4 hours Action Plan: 24 hours Resolve: 40 hours	\$500.00	\$500.00	\$1,000.00
Severity 4 – Low Respond: 4 hours Action Plan: 40 hours Resolve: 80 hours	\$250.00	\$250.00	\$500.00

IV. HOSTING ENVIRONMENT

A. General

93. MSDH is seeking a vendor hosted, cloud solution. The cloud hosted environment must be capable of supporting the solution without limit to user capacity as well as maintaining all database functions.
94. Vendor must submit a detailed description of their cloud hosting services. At a minimum, Vendor should address the following:
 - a. Retention scheme for standard server backups.
 - b. Plans for databases, applications, auto-run, and on-demand reporting, etc.
95. MSDH requires an at-most Recovery Time Objective (RTO) of 24 hours and an at-most Recovery Point Objective (RPO) of 24 hours. Cloud services must be restored within 24 hours of a service disruption. Production systems must be backed up at least nightly so that the longest possible period of data loss would be 24 hours. Vendor must describe how services meet or exceed these expectations.
96. Vendor must provide pricing details for cloud and application hosting services in Section VIII, Cost Information Submission which is found in RFP No. 4689.

Attachment A

RFP No. 4689 – WIC Text Messaging

B. Business Continuity/Disaster Recovery

97. So that MSDH can assess Vendor's business continuity strengths, Vendor must provide a preliminary business continuity plan that reveals Vendor's ability to analyze, design, implement, test, and maintain cloud services.
98. The business continuity plan must reveal contingency and disaster recovery strategies available to MSDH for the services sought by this RFP. At a minimum, the plan must address such questions and issues as:
 - a. What are your plans, procedures, and technical measures that will restore MSDH services as quickly and effectively as possible following a service disruption? So that MSDH can properly evaluate your response, provide as much detail as possible.
 - b. Is the distance between the backup facility and the primary facility adequate to ensure one incident does not affect both? Do the two sites provide redundant power and networking?
 - c. Describe your process for notifying MSDH when a major event has occurred or is likely to occur that will impact service? How do you keep your process and contacts updated?
 - d. Describe your plans for periodically testing business continuity and disaster recovery processes.
99. Upon award, the agreed upon RPO and RTO must be accounted for and documented in the resulting plans for business continuity and disaster recovery.

C. State of Mississippi Enterprise Cloud and Offsite Hosting Security Policy

100. Vendor understands and agrees that all proposed hosting services will comply with the State of Mississippi Enterprise Cloud and Offsite Hosting Security Policy specified below in this section of this RFP.
101. Per rule 1.4 of the State of Mississippi Enterprise Cloud and Offsite Hosting Security Policy, each agency must ensure that new contracts and amendments include the terms and conditions approved by ITS. The terms and conditions provided below are applicable for State of Mississippi data that the agency has categorized as public data.
102. Data Ownership: The State of Mississippi (State) shall own all right, title and interest in all data used by, resulting from, and collected using the services provided. The Service Provider shall not access State User accounts, or State 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 State's written request.
103. Data Protection: Protection of personal privacy and sensitive data shall be an integral part of the business activities of the Vendor to ensure that there is no inappropriate or unauthorized use of State information at any time. To this end, the Vendor shall safeguard the confidentiality, integrity, and availability of State information and comply with the following conditions
 - a. All information obtained by the Vendor under this contract shall become and remain the property of the State.

Attachment A

RFP No. 4689 – WIC Text Messaging

- b. At no time shall any data or processes which either belong to or are intended for the use of State or its officers, agents, or employees be copied, disclosed, or retained by the Service Provider or any party related to the Service Provider for subsequent use in any transaction that does not include the State.
104. Data Location: The Service Provider shall not store or transfer State data outside of the United States. This includes backup data and Disaster Recovery locations. The Service Provider will permit its personnel and contractors to access State data remotely only as required to provide technical support.
105. Encryption: The Vendor shall encrypt all non-public data in transit regardless of the transit mechanism.
106. For engagements where the Vendor 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 Vendor must describe existing security measures that provide a similar level of protection. Additionally, when the Vendor 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:
- a. The policy shall be issued by an insurance company acceptable to the State and valid for the entire term of the contract, inclusive of any term extension(s)
 - b. The Vendor and the State shall reach agreement on the level of liability insurance coverage required.
 - c. 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.
 - d. At a minimum, the policy shall include third party coverage for credit monitoring, notification costs to data breach victims, and regulatory penalties and fines.
 - e. The policy shall apply separately to each insured against whom claim is made or suit is brought subject to the Vendor's limit of liability.
 - f. The policy shall include a provision requiring that the policy cannot be cancelled without thirty (30) days written notice.
 - g. The Vendor shall be responsible for any deductible or self-insured retention contained in the insurance policy.
 - h. The coverage under the policy shall be primary and not in excess to any other insurance carried by the Vendor.
 - i. In the event the Vendor fails to keep in effect at all times the insurance coverage required by this provision, the State 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.
107. Breach Notification and Recovery: Unauthorized access or disclosure of non-public data is considered to be a security breach. The Vendor will provide immediate notification and all communication shall be coordinated with the State. When the Vendor or their sub-contractors are liable for the loss, the Vendor shall bear all costs associated with the investigation, response and recovery from the breach including

Attachment A

RFP No. 4689 – WIC Text Messaging

but not limited to credit monitoring services with a term of at least 3 years, mailing costs, website, and toll-free telephone call center services. The State shall not agree to any limitation on liability that relieves a Vendor from its own negligence or to the extent that it creates an obligation on the part of the State to hold a Vendor harmless.

108. Notification of Legal Requests: The Service Provider shall contact the State 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 the State. The Service Provider shall not respond to subpoenas, service of process, or other legal requests related to the State without first notifying the State unless prohibited by law from providing such notice.
109. Termination and Suspension of Service: In the event of termination of the contract, the Service Provider shall implement an orderly return of State data in CSV or XML or another mutually agreeable format. The Service Provider shall guarantee the subsequent secure disposal of State data.
 - a. Suspension of services: During any period of suspension of this Agreement, for whatever reason, the Service Provider shall not take any action to intentionally erase any State data.
 - b. Termination of any services or agreement in entirety: In the event of termination of any services or agreement in entirety, the Service Provider shall maintain the existing level of security as stipulated in the agreement and shall not take any action to intentionally erase any State data for a period of 90 days after the effective date of the termination. After such 90 day period, the Service Provider shall have no obligation to maintain or provide any State data and shall thereafter, unless legally prohibited, dispose of all State data in its systems or otherwise in its possession or under its control as specified in section 7(d) below. Within this 90-day timeframe, vendor will continue to secure and back up State data covered under the contract.
 - c. Post-Termination Assistance: The State 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.
110. Background Checks: The Service Provider shall conduct criminal background checks and not utilize any staff, including sub-contractors, to fulfill the obligations of the contract who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or any misdemeanor offense for which incarceration of a minimum of one (1) year is an authorized penalty. The Service Provider shall promote and maintain an awareness of the importance of securing the State's information among the Service Provider's employees and agents.
111. Security Logs and Reports: The Service Provider shall allow the State 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 of time 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 Vendor.

Attachment A

RFP No. 4689 – WIC Text Messaging

112. Contract Audit: The Service Provider shall allow the State to audit conformance including contract terms, system security and data centers as appropriate. The State may perform this audit or contract with a third party at its discretion at the State's expense.
113. Sub-contractor Disclosure: The Service Provider shall identify all of 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 Service Provider, who will be involved in any application development and/or operations.
114. Sub-contractor Compliance: Vendor must ensure that any agent, including a vendor or subcontractor, to whom the Vendor provides access agrees to the same restrictions and conditions that apply through this Agreement.
115. Processes and Procedures: The Service Provider shall disclose its non-proprietary security processes and technical limitations to the State so that the State can determine if and how adequate protection and flexibility can be attained between the State and the vendor. For example: virus checking and port sniffing — the State and the vendor shall understand each other's roles and responsibilities.
116. Operational Metrics: The Service Provider and the State shall reach agreement on operational metrics and document said metrics in the Service Level Agreement. Examples include but are not limited to:
 - a. Advance notice and change control for major upgrades and system changes
 - b. System availability/uptime guarantee/agreed-upon maintenance downtime
 - c. Recovery Time Objective/Recovery Point Objective
 - d. Security Vulnerability Scanning

V. IMPLEMENTATION REQUIREMENTS – STATEMENT OF WORK

A. Vendor Acknowledgement

117. This section outlines the minimum expectations of the awarded Vendor for implementation of the selected solution. Implementation deliverables will reveal the Vendor's expertise in project management, data conversion/migration, and acceptance testing, etc. MSDH expects the preliminary implementation plans to be refined by the awarded Vendor and MSDH project managers during the implementation process. Whether the awarded Vendor will need to be onsite at any time will be determined by the implementation project demands. MSDH reserves the right to require onsite Vendor participation if it would be in the best interest of MSDH.
118. The State expects the awarded Vendor to be responsible for design, configuration, implementation, testing, training, hosting, maintenance, and support of the awarded solution.
119. The State expects implementation with limited interruption to incumbent MSDH business operations. Any interruption to such operations must be approved by MSDH and conducted in a way to prevent loss of service.

Attachment A

RFP No. 4689 – WIC Text Messaging

120. Upon award, MSDH intends for the requirements set forth in RFP 4689, Attachment A to RFP 4689, and the awarded Vendor's proposal, including any subsequent, agreed upon provisions and revisions, to act as the Implementation Statement of Work.

B. Project Management Plan

121. Vendor must propose a project work plan that includes an implementation plan and schedule. The plan must include, but not be limited to, tasks (all phases), estimated hours per task, major project milestones, quality assurance checkpoints, etc. Provide an estimated timetable detailing all phases of implementation from the point of contract execution through completion of go-live, final system acceptance, and user training to MSDH staff and end users.
122. Upon award, the Vendor and MSDH will jointly modify the proposed plans as appropriate to meet implementation objectives. MSDH expects the Vendor to work with the MSDH Project Manager to ensure effective project management during all phases.
123. Vendor will be responsible for any integration or implementation issues that may arise during implementation.
124. As it relates to this procurement, Vendor must state all assumptions or constraints regarding the proposed solution and overall project plan, timeline, and project management.
125. Vendor must identify any potential risks, roadblocks, and challenges you have encountered in similar implementations that could negatively affect a timely and successful completion of the project. Vendor must recommend a high-level strategy that MSDH can take to mitigate these risks.
126. The implementation plan must include multiple environments, including Development, User Testing, Final Acceptance Testing, and Production. All customizations, integrations, and interfaces must be tested and validated.

C. Acceptance Test Plan

127. The Vendor must provide a proposed 'Acceptance Test Plan' (ATP) prior to implementation of the system. The ATP must show events, sequences and schedules required for acceptance of the system. MSDH must provide written approval that the proposed ATP is complete and acceptable.
128. MSDH personnel will conduct acceptance testing of the system after system testing has been completed and certified by the Vendor. The Vendor must participate in the acceptance testing of the system by providing technical staff at MSDH' office location to provide assistance in demonstrating all functions of the system. The system must be demonstrated to be operational by MSDH employees to ensure that proper training has been received.
129. The Vendor must agree to and allow for an acceptance period of 30 working days in accordance with the work plan delivery schedule.
130. The system must meet performance requirements as stated in this RFP. MSDH and the Vendor will mutually define the criteria for the performance test.
131. The Vendor must conduct an operational systems test of the proposed system and certify, in writing, that the system is ready for use and will perform in accordance with

Attachment A

RFP No. 4689 – WIC Text Messaging

the requirements stated in this document. The Vendor must ensure that the system operates in general according to MSDH specifications before turning the system over to MSDH. MSDH will not debug modifications for the Vendor.

132. Vendor agrees that upon the successful completion of all implementation phases, including end user training, MSDH will conduct a Final Acceptance Review (FAR) to determine whether or not Vendor has satisfied the terms and conditions of the awarded contract, which includes the requirements of RFP No. 4689, and Attachment A to RFP 4689.

D. Training Requirements

133. Vendor must provide training for all system users and administrators.
134. Training must be delivered through live virtual sessions.
135. Vendor must provide written user guides and all associated documentation and training materials including, but not limited to:
 - a. User manuals
 - b. Quick reference guides
 - c. FAQs
136. Vendor must ensure training is role-based, easy to understand, and accessible to users with varying technical skill levels.

VI. OTHER

A. Other Requirements

137. If any component(s) necessary for operation of the requested system is omitted from Vendor's proposal, Vendor must be willing to provide the component(s) at no additional cost.