THE STATE OF MONTANA
DEPARTMENT OF PUBLIC HEALTH AND HUMAN SERVICES

AMENDMENT NO. 2 TO MASTER AGREEMENT # 18091790020
Amendment to Maximus Human Services Master Agreement for Provider Services

This Amendment No. 2 ("Amendment") modifies, to the extent specified below, the terms and conditions of Master Agreement # 18091790020 (the "Contract") for the Provider Services entered into by and between the Department of Public Health and Human Services (the "Department"), 2550 Prospect Ave, Suite 200, Helena, MT 59601, and Maximus Human Services, Inc ("Contractor").

RECITALS

The purpose of this Amendment is to extend the term of the master contract and update references to the current CMS certification process and security requirements.

The terms of this Amendment are effective upon full execution of this Amendment.

This Master Agreement is amended as follows:

SECTION 2, TERM, will be amended as follows:

This Contract ~~includes a base contract period of seven (7) years, and may be extended for a total of three (3) additional years in one-year intervals if the parties agree to each one-year extension before the end of the then-current term of this Contract. The term of this Contract, including all extensions,~~ is effective from June 1, 2018 (the "Effective Date") through May 31, 2028, unless terminated pursuant to the provisions of this Contract. This Contract~~, including any extensions,~~ may not exceed a total of ten (10) years, at the option of the State.

Any Participating Addendum executed during the term of the Master Agreement may have a term of up to 10 years (120 months) from its Effective Date. The maximum expiration date of any Participating Addendum shall be 120 months from its Effective Date, unless otherwise restricted by applicable state law in the state executing the Participating Addendum or unless terminated in accordance with the terms of the Master Agreement.

The Term of a Participating Addendum includes the Participating Addendum base period, which consists of the mutually agreed-upon DDI duration (defined in months) plus the base operations duration of 4 years (48 months). The optional operations duration is the remainder of the total Participating Addendum Term, which is limited to 10 years, (calculated by subtracting both the DDI duration base period and the base operations duration from the 120-month maximum duration). The total duration of the Participating Addendum, including any extensions, shall not exceed 10 years. Any extension beyond the base period, including the optional operations duration, is at the discretion of the Participating State and shall be for a term most favorable to the Participating State.

Sections 24.8.1 through 24.8.5 remain unchanged. Section 24.8.6 is added to Section 24.8 Compliance with Civil Rights Laws as follows:

24.8.6 Nondiscrimination Against Firearms Entities/Trade Associations. Contractor shall not have a practice, policy, guidance, or directive that discriminates against a firearm entity or firearm trade association, and Contractor shall not discriminate during the term of the contract against a firearm entity or firearm trade association. This section shall be construed in accordance with 30-20-301, MCA.

APPENDIX C - ATTACHMENT F Requirements Response Matrix, requirements referencing security standards and MECT certification processes will be amended as follows (*The struck through requirements are formally removed from the scope and replaced with the replacement requirement number and requirement descriptions):*

Req ID	Requirement Description
~~CERT01~~ CERT17	The Contractor shall develop a Certification Crosswalk that describes how the Contractor's deliverables and other documentation align with federal certification requirements and ~~MECT~~ certification milestone reviews.
~~CERT02~~ CERT19	The Contractor shall complete milestone updates of the CMS Certification ~~Checklists~~ Criteria as requested by the State.
C~~ERT03~~ CERT20	The Contractor shall validate the system against the CMS Certification ~~Checklists~~ Criteria.
~~CERT04~~ CERT21	The Contractor shall contribute to the ~~quarterly IV&V certification reports~~ recurring project status and KPI reports required by CMS.
~~CERT05~~ CERT22	The Contractor shall provide staff resources to support ~~MECT milestone review and~~ certification activities including participating in planning activities, meetings and other activities as required by CMS.
~~CERT12~~ CERT23	The Contractor shall coordinate with the State to develop CMS Certification ~~Checklist~~ documentation for each ~~MECT Checklist requirement~~ Certification Criteria.
~~DOC02~~ DOC52	The Contractor shall develop and maintain a Certification Plan that defines the contractor's approach to CMS certification. It must describe the processes and procedures that will be used to manage Certification requirements. The Certification Plan must comply with the most current ~~MECT~~ CMS Certification process to ensure the system will meet all certification ~~requirements~~ criteria.
~~DOC01~~ DOC54	The Contractor shall develop, execute, maintain and deliver for the State's approval, a System Security Plan (SSP) that will document the current level of security controls within the module scope of work that protects the confidentiality, integrity and availability (CIA) of the solution and its information. This is a living document and will be updated no less than annually and when new vulnerabilities are identified and mitigated and when additional functionality and/or components are implemented. The System Security Plan must be approved before any State data is transferred or entered into the solution. The State must approve all revisions of the System Security Plan. If the Contractor's solution is hosted by the State, the State will provide supporting information to the Contractor to complete the SSP. The SSP must address the following topics: • Adherence to the State's requirements outlined in the "Security and Privacy Controls Requirements" document, included in the Procurement Library; • Compliance with the Centers for Medicare and Medicaid Services (CMS) Acceptable Risk Safeguards (ARS) to assess CIA and NIST SP 800-53 Rev 4, or the most recent version required by CMS, at a "moderate" control level;

Req ID	Requirement Description
	• Data center physical security; • Network segmentation • Application security and data sensitivity classification, including Protected Health Information (PHI) and Personally Identifiable Information (PII); • End-point protections such as multiple redundant firewalls and host-based intrusion detection systems; • Identification and prevention of the use of prohibited functions, ports, protocols, and services; • Network, firewall, server and other security-related configurations and changes; • Intrusion detection and prevention; • Network scanning tools; • Host hardening; • Internet filtering; • Remote access; • Encryption of data at rest and in transit; • User authentication and directory services; • Interfaces and exchange of data with external entities; • System penetration testing; • Management of operating system and security patches; • Anti-Virus and malware detection and email gateways; • Assessment and testing of system and code modifications; and • Allowable internal and external communication protocols. • Compliance with the Federal Risk and Authorization Management Program (FedRAMP) Certification, FedRAMP Risk Assessment that indicates compliance or documented NIST 800-53 rev 4, or the most recent version required by CMS, at a “moderate” system risk assessment designation for Contractor hosted solutions; • Compliance with Statement on Standards for Attestation Engagements (SSAE-~~18~~ 22) SOC 2 Type 2.
~~DOC41~~ DOC55	The Contractor shall provide a Deliverable Expectations Document (DED) for each deliverable that describes the purpose, content, ~~applicable MECT minimum required content~~ alignment with federal certification guidance and industry standards (e.g., PMI, IEEE/ISO, CMS XLC) that are satisfied for each Deliverable. Each DED is a deliverable.
~~DOC46~~ DOC56	The Contractor shall provide a User Interface Style Guide or equivalent document defining the design standards for user interfaces. The User Interface Style Guide must demonstrate how the solution meets the most current ~~MECT~~ federal certification user interface requirements including: a. User ability to customize or make adjustments (e.g. language support, font size) to portal presentation. b. Users utilizing scripting languages and/or assistive technology have the ability to access the information, field elements, and functionality required for electronic form or page completion and submission including directions and cues. c. User Interface organization so documents are readable without requiring an associated style sheet. d. User Interfaces identifying row and column headers for data tables. e. User Interfaces informing users when a timed response is required and given sufficient time to indicate more time is required. f. User Interfaces providing a method that permits users to skip repetitive navigation links. g. User Interfaces provide text titles for frames to facilitate frame identification and navigation. h. User Interfaces use markup to associate data cells and row/header cells for data tables that have two or more logical levels of row or column headers.
~~INT40~~ INT100	The Contractor shall provide technical, functional and performance documentation required by ~~the IV&V Contractor for the solution in order to support IV&V reporting needs~~

Req ID	Requirement Description
	~~identified in the most current version of MECT~~ CMS for certification and ongoing compliance.
~~KR29~~ KR44	The Contractor's Certification Lead must meet the following qualifications including: a. Minimum of three (3) years experience certifying systems against industry standards for projects similar in size and scope to this project. b. In-depth understanding of the most current ~~MECT~~ certification ~~lifecycle required~~ process and requirements to successfully validate the system.
~~RQM03~~ RQM09	The Contractor shall document any gaps between the initially configured solution and the business requirements in the requirements management tool. Gaps must show bi-directional traceability with applicable business requirement(s), design, test cases, test results, ~~MECT~~ certification criteria and certification artifacts.
~~RQM06~~ RQM10	The Contractor shall develop, maintain and submit a Requirements Traceability Matrix (RTM) to show bi-directional traceability with applicable business requirements and their realization throughout all project phases (e.g., requirements, design, testing and certification ~~(MECT) checklist items~~ requirements). This should include how the requirement is realized (e.g., configuration, custom development, base functionality). All revisions must be reviewed and approved by the State.
~~RQM07~~ RQM11	The Contractor's requirements management tool shall have the ability to manage requirements traceability by module(s), MITA business area, MITA business process and ~~MECT checklists~~ federal certification criteria.
~~ENV04 or ENV08~~ ENV12	The Contractor's hosting environment for all module components shall be compliant with Statement on Standards for Attestation Engagements (SSAE~~-18~~ 22) SOC 2 Type 2 and has Federal Risk and Authorization Management Program (FedRAMP) Certification, FedRAMP Risk Assessment that indicates compliance, or has a documented NIST 800-53 rev 4, or the most recent version required by CMS, at a "moderate" system risk assessment designation. If the Contractor proposes either a multi-tenant solution or a public cloud, hybrid cloud (Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS)), or community cloud ~~enviornment~~ environment, the vendor must ensure that the environment is either FedRAMP certified or that the shared resources are only accessible by HIPAA-covered entities as defined in 45 CFR 160.103.
~~SEC15~~ SEC90	The Contractor shall provide an independent third party to perform penetration testing within six (6) months prior to implementation. Penetration testing must also be performed by an independent third party on an annual basis and when additions or changes to functionality impact the security framework, architecture or when a new vulnerability exists. Penetration Test Report results shall be supplied to the Department and any major or critical vulnerabilities mitigated. The Penetration Test Report is part of the independent third party security assessment required by CMS and must be conducted by a fully independent third party as defined by CMS.
~~SEC19~~ SEC84	The Contractor's data encryption solution shall meet Federal Information Processing Standard (FIPS) 140-2, ~~and at a minimum use AES 128 encryption~~ be in compliance with FIPS 140-3 no later than September 21, 2026, and at a minimum use AES 256 encryption for data at rest and TLS 1.2 for data in transit.
~~SEC22 or SEC85~~ SEC89	The Contractor will provide a completed Security Audit Report with results to the Department by the 30th (thirtieth) of September each year. The Security Audit Report must include either an electronic data processing (EDP) systems audit using SSAE ~~-18~~ 22 at a minimum level service organization control (SOC) 2 Type II or a NIST 800-53 rev 4, or the most recent version required by CMS, assessment at a "moderate" system risk control level. The Security Audit Report is part of the independent third party security assessment required by CMS and must be conducted by a fully independent third party as defined by CMS.
~~SEC51~~ SEC86	The Contractor shall comply with the current standard for NIST Federal Information Processing Standards (FIPS) Publication 180-4: Secure Hash Standards as required by CMS for use of secure hash algorithms. Contractor must comply with a subsequent standard no later than the NIST-identified retirement date for 180-4.

Req ID	Requirement Description
~~SEC52~~ SEC87	The Contractor shall comply with NIST Federal Information Processing Standards (FIPS) Publication 186-~~4~~ 5: Digital Signature Standard as required by CMS for use of secure algorithms in digital signatures.
~~SEC53~~ SEC88	The Contractor shall comply with the current version of Harmonized Security and Privacy Framework - Exchange Reference Architecture Supplement ~~Version 1.0~~ and as required by CMS.
SEC76	The Contractor's mobile application shall meet FIPS 140-2 standard for security, and be in compliance with FIPS 140-3 no later than September 21, 2026.
~~SLA51~~ SLA172	Contractor will ensure that Module Federal Certification is achieved retroactive to the first day of Operations and continued throughout the Operations Phase. The Contractor is responsible for meeting the Federal standards, conditions and business requirements, formally published by CMS on the date the RFP closes, necessary to ensure initial and continued federal Certification for the operation of the Module and Department to receive full Federal Financial Participation (FFP) and the Federal Medical Assistance Percentage (FMAP) funding. In addition, the Contractor is responsible for meeting any new or modified Federal standards necessary to ensure initial and continued federal Certification, provided that to the extent those standards or requirements are not outside the scope of the RFP and do not result in a material cost impact on Contractor, otherwise the Contractor shall only be required to meet them if and to the extent the parties agree to do so through the Change Order process. Contractor will provide all support requested by the Department during Certification and any recertification conducted by CMS and by the Department. The support will include assisting the Department and CMS in developing artifacts and evidence to support the Certification review. This includes developing the Certification presentation and participation in the Certification review and all activities needed for preparation of Certification. Liquidated damages: Contractor must pay the Department the actual damages incurred by the Department related to the Module DDI and Certification, if CMS does not fully compensate the Department at the maximum allowable FFP rate and the FMAP for the Module as delivered by the Contractor. The actual damages are the difference between the total of the sums of monies actually received from CMS by the Department and the total of the sums of monies that could have been received by the Department at maximum allowable FFP and the FMAP rate.

All other Attachment F requirements remain unchanged.

All other provisions of the Master Agreement are unchanged, and it is further the intent of the parties that any inconsistent provisions not addressed by the above Amendment are modified and interpreted to conform to this Amendment No. 2.

(Rest of page intentionally left blank.)

MONTANA DEPARTMENT OF PUBLIC HEALTH AND HUMAN SERVICES

BY: DocuSigned by: Rebecca de Camara 4199A8B71A6E474... Date: 5/29/2025

Rebecca de Camara, Medicaid and Health Services Executive Director

BY: Signed by: Charles Brereton F85D511C51B4408... Date: 5/30/2025

Charles T. Brereton, Director

BY: DocuSigned by: Carrie Albro EB17B5BD9AD949B... Date: 5/27/2025

Carrie Albro, Chief Information Officer

MONTANA DEPARTMENT OF PUBLIC HEALTH AND HUMAN SERVICES, OFFICE OF LEGAL AFFAIRS

Approved as to Legal Content:

BY: DocuSigned by: Mark Prichard 6EA698E1E676459... Date: 5/23/2025

Attorney

MONTANA DEPARTMENT OF ADMINISTRATION, STATE PROCUREMENT SERVICES DIVISION

Approved as to Form:

BY: Signed by: Nolan Harris B31066F651454E1... Date: 5/23/2025

SPSD, Contract Officer

Contractor is notified that pursuant to 2-17-514, MCA, the Department of Administration retains the right to cancel or modify any contract, project or activity that is not in compliance with the Agency's Plan for Information Technology, the State Strategic Plan for Information Technology or any statewide IT policy or standard.

BY: DocuSigned by: Kevin Gilbertson 2D9081032F49415... *Date:* 5/23/2025

Kevin Gilbertson, State Chief Information Officer

ITPR# 13203_202557113928

CONTRACTOR

BY: Signed by: Austin Raluskopf F05B14FA700D4E7... Date 5/29/2025