



February 15, 2023

Dear Legislators,

This letter and attached documents are being sent to you in accordance with Minnesota Statute 62V.05, subdivision 12. The attached documents contain all interagency agreements and intra-agency transfers occurring during the 2nd quarter of FY23. As required under Minnesota Statute 62V.05, subdivision 12, this report includes:

- “(1) interagency agreements or service-level agreements and any renewals or extensions of existing interagency or service-level agreements with a state department under section 15.01, state agency under section 15.012, or the Office of MN.IT Services, with a value of more than \$100,000, or related agreements with the same department or agency with a cumulative value of more than \$100,000; and
- (2) transfers of appropriations of more than \$100,000 between accounts within or between agencies.”

Included within this report are copies of all interagency agreements and service level agreements to which MNsure was a party during the 2nd quarter of FY23.

Thank you for the opportunity to share this information. Please direct any questions you might have to Pete Engler, Government Affairs Manager, at 651.247.0247 or [Pete.Engler@state.mn.us](mailto:Pete.Engler@state.mn.us)

Sincerely,

A handwritten signature in blue ink, appearing to read "Nathan".

Nathan Clark  
Chief Executive Officer



**MNsure - 62V.05 subd. 12**

FY 2023 Quarter 2 MNsure Interagency Agreements and Service Level Agreements

Q2 Ending Dec 31, 2022

Agency	Amount	Legal Authority	Purpose	Effective Date	Duration
MNIT	\$ 414,345	M.S. 16E.016, 62V.05	MNIT provides enterprise IT services to MNsure *reflects actual costs paid to date	7/1/2019	ongoing
DHS	\$ 7,358,172	M.S. 62V.05, 471.59	MNsure contracts with DHS to provide services as described in the IAA	10/1/2021	6/30/2023
MNsure	\$0	Public Law 89-97 Title XIX	DHS contracts with MNsure for MNsure participation in the administration of the MN State Plan. *reflects actual costs paid to date.	10/1/2021	6/30/2023
MNsure	\$ 13,269,000	General Fund	MNsure received a transfer from the General Fund for reinsurance	State Fiscal Year 2023	N/A
<b>Total</b>	<b>\$ 21,041,517</b>				

## **STATE OF MINNESOTA INTERAGENCY AGREEMENT**

**WHEREAS**, the Minnesota Department of Health (MDH), the Minnesota Department of Commerce (Commerce) and (MMB), as agency for the Minnesota Insurance Marketplace established under Minnesota Laws 2013, Chapter 9 (MNsure) (collectively, "the Agencies") are authorized to enter into this Agreement pursuant to law, including by Minnesota Statutes, § 471.59, subdivision 10; and

**WHEREAS**, Public Law 111-148, known as the Patient Protection and Affordable Care Act (ACA) and rules promulgated thereunder have a number of provisions pertaining to the regulation subject to the jurisdiction of the Agencies; and

**WHEREAS**, Executive Order 11-30 directed the design and development of a Minnesota Health Insurance Exchange to achieve greater access to affordable, high-quality health coverage that maximizes consumer choice and minimizes adverse selection; and

**WHEREAS**, MMB was recently designated to be the lead agency in the design and development of MNsure/Minnesota Insurance Marketplace; and

**WHEREAS**, MMB (or its predecessor, Department of Commerce) has been awarded multiple Health Insurance Exchange Level 1 Establishment Grants by the U.S. Department of Health and Human Services through a Health Insurance Exchange Level 1 Establishment Grant Agreement to design and develop a Minnesota Health Insurance Exchange (Exchange) that includes enrollment, eligibility, small business health options program, plan comparison and provider information, fund aggregation and account management functions that have financial impacts across multiple agencies; and

**WHEREAS**, Minn. Stat. § 62V authorizes the establishment of MNsure/Minnesota Insurance Marketplace; and

**WHEREAS**, the ACA requires every plan sold through MNsure/Minnesota Insurance Marketplace to be certified as a Qualified Health Plan (QHP) or as a "qualified dental plan" (QDP) before being offered for sale by the MNsure/Minnesota Insurance Marketplace; and

**WHEREAS**, the ACA provides that the Secretary of the United States Department of Health and Human Services (HHS) shall, by regulation, establish the criteria for certification of health plans as QHPs and QDPs and specifies certain criteria to be included in such certification; and

**WHEREAS**, MNsure/Minnesota Insurance Marketplace is authorized to certify health plans as QHPs or dental plans as QDPs under Minn. Stat. § 62V.05, subd. 5(c) according to applicable certification requirements.

**WHEREAS**, the Agencies have expertise in and jurisdiction over certain requirements included

in the mandated QHP certification process; and

**WHEREAS**, Minnesota law authorizes MDH to issue certificates of authority to Health Maintenance Organizations (HMOs) following review of network adequacy, quality assurance and improvement standards, enrollee rights and other requirements; and

**WHEREAS**, MDH is required to create and annually update a set of measures by which to assess the quality of health care services offered by health care providers and issue annual public reports on provider quality, and to develop and publish reports on provider cost and quality through the Provider Peer Grouping system; and

**WHEREAS**, Minnesota law directs MDH to conduct data and research initiatives focused on monitoring and improving the efficiency and effectiveness of Minnesota health care (Minn. Stat., § 62J.301) and to evaluate the impact of health reform activities (Minn. Stat. § 62J.311); and

**WHEREAS**, Commerce enforces laws relating to insurance in the State of Minnesota, including but not limited to those relating to insurer certificates of authority, licensure, solvency, rates, benefit forms, marketing and consumer protection; and

**WHEREAS**, the Agencies hold a shared interest in collaborating in the development and implementation of the MNsure/Minnesota Insurance Marketplace, including ensuring that QHPs and QDPs offered through MNsure/Minnesota Insurance Marketplace meet federal and state laws and regulations including but not limited to licensing, network adequacy, and service area standards, evaluating the impact of MNsure/Minnesota Insurance Marketplace on the health insurance market, and in developing options for publicly reporting quality and provider peer grouping information in a consumer-friendly manner on a single, one-stop shopping website while maintaining all relevant administrative and data management rights and regulatory oversight obligations; and

**WHEREAS**, it is the intent of this Agreement to memorialize the Agencies' joint effort and establish the process by which QHP and QDP certification will take place for plans sold within MNsure/Minnesota Insurance Marketplace; and

**WHEREAS**, the Health Insurance Exchange Level 1 Establishment Grant Agreement requires, among other items, funding for the Agencies' staff, contracts and support costs for activities associated with the establishment and implementation of MNsure/Minnesota Insurance Marketplace; and

**WHEREAS**, the Minnesota state accounting system (SWIFT) budgetary and financial management role-based security can be utilized for multiagency access to financial department IDs (FINDEPT IDs) for the purpose of allocating and managing approved federal grants across multiple agencies; and

**WHEREAS**, it is the desire of agencies impacted by the federal Establishment grants to allow each agency to direct charge approved costs and not implement an invoice and payment process

across agencies, as described in this agreed-upon approach:

- Interagency work group plans and approves the state-wide MNsure/Minnesota Insurance Marketplace Project budget, by funding source, and by agency SWIFT expense budget FINDEPT ID.
- FINDEPT ID expense budgets are established in SWIFT only after all applicable federal CCIIO grant award, federal CMS cost allocation, and Minn. Stat. § 3.3005 approvals are obtained.
- Agency responsibility for establishing and maintaining the FINDEPT ID expense budgets in SWIFT corresponds to the underlying funding source. For example, MMB is responsible for entry in SWIFT of the FINDEPT ID expense budgets that are funded by the federal CCIIO grants.
- As an alternative to an interagency billing process, the interagency work group authorizes SWIFT security access to be granted to a limited number of employees at each agency so SWIFT accounting transactions, inquiries and reports may be processed directly against these FINDEPT IDs.

**NOW, THEREFORE,** it is agreed:

## **1. Term of Agreement**

**1.1 Effective date:** March 15, 2013 or the date the State obtains all required signatures under Minn. Stat. § 16C.05, subd. 2, whichever is later.

**1.2 Expiration date:** This Agreement shall remain in effect until any party hereto chooses to terminate upon thirty days written notice to all parties to the Agreement.

**1.3** The following definitions apply to this Agreement:

- i. **Exchange Interagency Subcabinet** is the group that is charged with: effectively executing design, development, and implementation activities for the MNsure/Minnesota Insurance Marketplace that involve multiple agencies; creating an efficient process for decision-making and issue resolution; and establishing clear communication, coordination, project management, and documentation mechanisms. It is chaired by MMB Commissioner Schowalter, or his successor; staffed by Nathan Morocco, or his successor; and includes Commissioners from the Department of Human Services (DHS), Department of Commerce (Commerce), Department of Health (MDH), Office of Enterprise Technology d/b/a MNIT Services (MN.IT), and Administration (Admin); and select MNsure/Minnesota Insurance Marketplace steering members and senior staff, as needed.
- ii. **FINDEPT ID (SWIFT Financial Department IDs)** is the 8-character code that identifies the specific budget from which payments are made.
- iii. **Indirect Costs** are all general support costs that cannot be directly charged to any agency program.
- iv. **Procurements** include: Requests for Proposals (RFPs), Contracts (both

Professional/Technical and grant contracts), Master Professional/Technical Service Contracts, Statements of Work (SOWs), Work Orders (WOs), and the purchase of Goods and Services.

- v. **SWIFT** is the Statewide Integrated Financial Tools system.
- vi. **Travel Costs** refers to reimbursement for travel and subsistence expenses actually and necessarily incurred, which must be in no greater amount than provided in the current Bargaining Units Agreements or the “Commissioners Plan” published by MMB, whichever is appropriate.

## **2. Duties of the Parties**

### **2.1 MMB/MNsure/Minnesota Insurance Marketplace Shall:**

- 2.1.1 Delegate authority for review and approval of certain components identified in this Interagency Agreement of QHP/QDP certification, recertification, and decertification processes to Commerce and MDH and compensate Commerce and MDH for these services in accordance with the terms of this Agreement.
- 2.1.2 Seek funding as appropriate to continue the design, development, and implementation of the MNsure/Minnesota Insurance Marketplace, including a module incorporating the display of MDH quality and provider peer grouping information in a user-friendly way. In seeking that federal funding, MMB shall collaborate with partner agencies and be cognizant of the impact that its creation and development have on both existing and future work of its partner agencies. MNsure/Minnesota Insurance Marketplace shall work with MDH to plan and implement user/usability testing activities related to the Provider Display Module and to establish a process for review and approval of provider peer grouping data prior to publishing to the display.
- 2.1.3 Fulfill the following financial management duties:
  - i. Create separate SWIFT FINDEPT IDs and budgets under each federal Establishment grant as outlined in Exhibits A and B. FINDEPT IDs shall be created to meet the needs of both MNsure/Minnesota Insurance Marketplace and the Agencies.
  - ii. Ensure cash draws and quarterly federal financial reports are processed in a timely manner to meet the needs of MNsure/Minnesota Insurance Marketplace and the Agencies.
  - iii. Obtain any and all necessary approvals/Gate Reviews required by the Center for Consumer Information and Insurance Oversight (CCIIO).
  - iv. Initiate the creation of an interagency workgroup to review SWIFT security roles for the project, review grant allocations including mid-year and end of year reallocations and other financial management processes needed to administer the multiagency financing of MNsure/Minnesota Insurance Marketplace.
  - v. The MMB staff who is authorized and has the ability through role-based

security in SWIFT to establish and adjust budgets in the SWIFT FINDEPT ID is Jackie Miller or her successor. This activity will be reported monthly and monitored by Barb Juelich or her successor, and by the interagency work group pursuant to IV. Changes in authorized staff including additional staff or replacement staff shall be communicated to all appropriate agency authorized representatives.

- 2.1.4 Manage any appeals related to QHP/QDP certification or decertification, including initiating, as appropriate, a contested case proceeding as required under Minn. Stat. § 62V.05, subd. 6.
- 2.1.5 In collaboration with Commerce, carry out and/or enforce provisions of 45 C.F.R. §§ 156.285 and 156.290 (exchange notification only).

## **2.2 MDH shall:**

- 2.2.1 Collaborate with MNSure/Minnesota Insurance Marketplace staff in the development of the Provider Display module, including:
  - i. Determine that quality and peer grouping data and other content related to this data are accurate and ready to be publicly reported;
  - ii. Develop and maintain a database data dictionary, and other supporting materials for quality and peer grouping data and provide content expertise on the organization of this data;
  - iii. Transfer test files of summary data on health care provider quality and peer grouping, and other data files, to MNSure/Minnesota Insurance Marketplace staff or contractors as necessary for development of the functionality of the Provider Display Module. Information transferred shall be summary level data files representing a sample of facilities, and shall not include any individual private data. MDH shall clearly indicate that data are to be used for testing purposes only;
  - iv. Transfer production files of summary data on health care provider quality and peer grouping to MNSure/Minnesota Insurance Marketplace staff or contractors consistent with a schedule agreed upon by MDH and MNSure/Minnesota Insurance Marketplace. MDH shall attest to the quality and readiness of the data prior to sending to MNSure/Minnesota Insurance Marketplace.
  - v. Participate in meetings with MNSure/Minnesota Insurance Marketplace staff and contractors regarding use/interpretation of quality and provider peer grouping information, display options, content, timelines, and other relevant issues;
  - vi. Participate in the planning and implementation of user/usability testing activities related to the Provider Display module;
  - vii. Provide input to MNSure/Minnesota Insurance Marketplace staff on potential improvements to Provider Display module functionality,

- viii. appearance, and content; and Review and troubleshoot issues related to module functionality, administrative functions, security, and other technical issues.
  - ix. Work with MNSure/Minnesota Insurance Marketplace staff on providing assistance and technical expertise to create a crosswalk to link quality and peer grouping data to the MNSure/Minnesota Insurance Marketplace provider directory.
- 2.2.2 Provide cross-agency technical assistance to ensure proper use and understanding of data provided by MDH to MNSure/Minnesota Insurance Marketplace contractors.
- 2.2.3 With input from MNSure/Minnesota Insurance Marketplace and Commerce staff, develop and implement a framework for evaluation of the impact of the MNSure/Minnesota Insurance Marketplace on the Minnesota insurance and health care markets.
- 2.2.4 Provide representatives for the MNSure/Minnesota Insurance Marketplace project management structure including the steering committee and technical workgroups.
- 2.2.5 Consistent with the requirements of 45 C.F.R. § 155.1010, in addition to all other regulatory responsibilities, collaborate with Commerce and the MNSure/Minnesota Insurance Marketplace on the QHP/QDP certification, recertification and decertification processes. MDH will ensure sufficient staffing/and or qualified contractor resources are in place to carry out the following duties by August 1 of each year, including but not limited to such duties as:
  - i. **Licensure.** Confirm with the MNSure/Minnesota Insurance Marketplace that carriers seeking to participate in the MNSure/Minnesota Insurance Marketplace subject to MDH's regulatory jurisdiction are licensed consistent with relevant provisions of Minnesota Statutes.
  - ii. **QHP Issuer Benefit Information.** At least annually for plans filed subject to MDH's regulatory jurisdiction, review plan-covered benefits and cost-sharing requirements submitted by issuers via System for Electronic Rate and Form Filing (SERFF). Such review will be made to ensure all ACA requirements are met, including but not limited to:
    - 1. Essential Health Benefits are included.
    - 2. Limitations on cost sharing are met.
    - 3. Ensure benefit design is not discriminatory



- iii. **Network Adequacy.** Review provider network filings submitted by issuers as part of the certification process for the MNsure/Minnesota Insurance Marketplace.
- a) Conduct detailed analysis to determine if the proposed provider network(s) is adequate in terms of numbers, locations and types of providers, including mental health and substance abuse providers, to ensure that all services are accessible without unreasonable delay throughout the QHP/QDP's service area.
  - b) Review will apply the standards of Minn. Stat. § 62D.124 and Minn. Rules chapter 4685.3300, subpart 9.
  - c) Analysis must include review of any adequacy standards contained in the ACA and federal Exchange regulations as well as in Minnesota law and rules.
  - d) Review and approve or deny all requests for a waiver submitted by an issuer.
  - e) Update the status of the proposed provider network(s) via the SERFF database.
  - f) Reviews will be completed within 90 days of receipt of the network filing or by August 1 of each year.
  - g) Review provider termination notices to determine if any termination will cause the QHP's provider network to no longer meet network adequacy standards. If so, notify MNsure/Minnesota Insurance Marketplace of this determination.
  - h) Require the issuer to file its plan for addressing the network insufficiency with MDH, including notification letters, waiver requests and continuity of care information; monitor the plan and inform MNsure/Minnesota Insurance Marketplace when the network has been corrected. Should the network insufficiency not be corrected, notify MNsure/Minnesota Insurance Marketplace that the network no longer meets adequacy standards of state law.
  - i) Review all service area expansions submitted by issuers to determine if the QHP provider network will be adequate in terms of numbers, locations and type of providers.
  - j) Review all waiver requests to determine if a waiver from network adequacy standards should be granted.
  - k) Review networks for participation by Essential Community Providers consistent with Minn. Stat. § 62Q.19, and 45 CFR § 156.235
- iv. **Services Areas.** Conduct the review of proposed service areas for each QHP/QDP to be offered on MNsure/Minnesota Insurance Marketplace.
- a) Inform issuers of any supplemental material including maps that must be filed for proposed service areas in addition to data included on the standard template available through SERFF.

- b) Consistent with section 2.2.8 of this Interagency Agreement, work with MNsure/Minnesota Insurance Marketplace staff to determine how MDH will evaluate service area filings to ensure proposed service areas meet certification criteria in 2c, 2d, and 2e below.
- c) Notify issuers that the proposed service area filing must contain an affirmative showing that the service area is being established without regard to racial, ethnic, language, health-status, or other factors that exclude specific high utilizing, high cost or medically-underserved populations.
- d) For each proposed service area, using the identified standards, determine if each QHP has been established without regard to racial, ethnic, language, health status-related factors specified under section 2705(a) of the PHS Act, or other factors that exclude specific high utilizing, high cost or medically underserved populations.
- e) For each proposed service area that is smaller than one county, notify issuers that the filing must contain an affirmative showing that the smaller service area is necessary, nondiscriminatory, and in the best interest of the qualified individuals and employers.
- f) Update the status of each proposed service area in SERFF to indicate whether the service area meets or does not meet all of the minimum criteria under the ACA.

v. **Other functions.** Carry out and/or enforce the provisions of 45 C.F.R. §§ 156.210, 156.225 (benefit design), 156.250, and 156.280 for plans subject to MDH jurisdiction. Carry out and/or enforce the provisions of 45 C.F.R. §§ 156.230, 156.235, 156.245, 156.275, and 156.295.

2.2.6 On an annual basis and in coordination with Commerce, review written attestations and other submissions made by carriers submitted through an established recertification process and provide determinations to the MNsure/Minnesota Insurance Marketplace on whether certification criteria reviewed by MDH continue to be met. These determinations must be made by August 1 of each year.

2.2.7 Provide technical assistance to MNsure/Minnesota Insurance Marketplace in appeals related to decertification/non-certification of a QHP/QDP under Minn. Stat. § 62V.05, subd. 6., to the extent decertification of a QHP or QDP is based on a determination of one or more certification criteria evaluated by MDH, assist the MNsure/Minnesota Insurance Marketplace in the appeal process.

- 2.2.8 To the extent the federally required certification process involves functions or aspects of functions that extend beyond current Commerce and MDH statutory authority, consult with the MNsure/Minnesota Insurance Marketplace prior to carrying out its review process to ensure mutual understanding and agreement on the application of a particular policy.
- 2.2.9 Provide project management services for MDH duties outlined in this section.
- 2.2.10 Fulfill the following financial management duties:
- i. Participate in the interagency workgroup identified in Section 2.1.3.
  - ii. Administer SWIFT multi-agency FINDEPT IDs with approved security access.
  - iii. Allow MMB access to FINDEPT IDs according to security roles established by the interagency workgroup.
  - iv. Obtain approval for procurements from the MNsure/Minnesota Insurance Marketplace with the exception of general supplies, computers and similar equipment for approved staff, and other general administrative support costs such as rent, communications, and network access.
  - v. Assign approved staff to appropriate FinDept for funding.
  - vi. Obtain approval from MNsure/Minnesota Insurance Marketplace for assigning staff costs to FinDept when the position was not included in the grant.

### 2.3 Commerce shall:

- 2.3.1 Consistent with the requirements of 45 C.F.R. § 155.1010, in addition to all other regulatory responsibilities, and prior to the beginning of the relevant open enrollment period, collaborate with MDH and MNsure/Minnesota Insurance Marketplace on the QHP/QDP certification, recertification and decertification process. Commerce will ensure sufficient staffing/and or qualified contractor resources are in place to carry out the following duties by August 1 of each year:
- i. **Licensure.** Confirm with MNsure/Minnesota Insurance Marketplace that carriers seeking to participate in MNsure/Minnesota Insurance Marketplace subject to Commerce's regulatory jurisdiction are licensed consistent with relevant provisions of Minnesota Statutes.
  - ii. **QHP Issuer Rate and Benefit Information.** Review plan rates, covered benefits, and cost-sharing requirements submitted by issuers via the System for Electronic Rate and Form Filing (SERFF) at least annually. Such review will be made to ensure ACA requirements are met, including, but not limited to the following:
    1. Essential Health Benefits are included.
    2. Limitations on cost sharing are met.

3. Actuarial value/metal level requirements are met.
  4. Ensure benefit design is not discriminatory.
- iii. **Marketing practices.** Ensure applicable state laws are met regarding marketing by health plan issuers and that marketing practices do not discourage enrollment of persons with significant health needs.
  - iv. **Other functions.** Carry out and/or enforce the provisions of 45 C.F.R. §§ 156.210, 156.225 (benefit design), 156.250, 156.280, and 156.290 for plans subject to Commerce jurisdiction. Carry out and/or enforce the provisions of 45 C.F.R. §§ 156.220, 156.225 (marketing), 156.250, 156.255, 156.260, 156.265, and 156.270. In collaboration with MNsure/Minnesota Insurance Marketplace, carry out and/or enforce the provisions of 45 C.F.R. §§ 156.285 and 156.290.
- 2.3.2 Determine access rights to SERFF under existing contract relations and provide access to MDH within agreed upon parameters.
  - 2.3.3 Where required under federal rules, collect information on transparency measures described in 45 C.F.R. § 156.220 from QHP/QDP issuers in accordance with the ACA and any further regulations or guidance issued by the United States Department of Health and Human Services on these reporting requirements.
  - 2.3.4 On an annual basis and in coordination with MDH, review written attestations and other submissions made by carriers submitted through an established recertification process and provide determinations to MNsure/Minnesota Insurance Marketplace on whether certification criteria reviewed by Commerce continue to be met. These determinations must be made by August 1 of each year.
  - 2.3.5 To the extent the federally required certification process involves functions or aspects of functions that extend beyond current Commerce statutory authority, consult with MNsure/Minnesota Insurance Marketplace prior to carrying out its review process to ensure mutual understanding and agreement on the application of a particular policy.
  - 2.3.6 Fulfill the following financial management duties:
    - i. Participate in the interagency workgroup identified in Section 2.1.3.
    - ii. Administer SWIFT multi-agency FINDEPT IDs with approved security access.
    - iii. Allow MMB access to FINDEPT IDs according to security roles established by the interagency workgroup.
    - iv. Obtain approval for procurements from MNsure/Minnesota Insurance Marketplace with the exception of general supplies, computers and similar equipment for approved staff, and other general administrative support costs such as rent, communications, and network access.

- v. Assign approved staff to appropriate FinDept for funding.
- vi. Obtain approval from MNSure/Minnesota Insurance Marketplace for assigning staff costs to FinDept when the position was not included in the grant.

2.3.7 Provide technical assistance to MNSure/Minnesota Insurance Marketplace in appeals related to the decertification/non-certification of a QHP/QDP under 62V.05, subd. 6, to the extent the decertification/non-certification of an issuer, QHP or QDP is based on one or more of the certification criteria evaluated by Commerce.

## **2.4 All Parties shall:**

- 2.4.1 Participate with other agencies in an interagency workgroup identified in Section 2.1.3. The workgroup shall:
- i. Review the monthly reports regarding transfer of funds within and among all accounts to ensure accuracy.
  - ii. Be the first level hearing to resolve any disputes regarding these accounts.
  - iii. Escalate any disputes that cannot be resolved at this level to the Exchange Interagency Subcabinet.
  - iv. Recommend roles and responsibilities between the MN sure/Minnesota Insurance Marketplace and other agencies related to the financial management and budget operations of federal Establishment grants.
  - v. Recommend SWIFT security roles to be utilized as part of the multi-agency financial management and budget operations of the federal Establishment grants.
  - vi. Recommend mid-year and end of year reallocation of federal Establishment grants.
  - vii. Review business process issues with the SWIFT security roles implemented and recommend adjustments.
  - viii. The workgroup shall report its findings and recommendations to designated leadership in the MNSure/Minnesota Insurance Marketplace Multi-Agency Governance Structure.
- 2.4.2 Participate in audit or compliance activities necessary to meet any federal or state oversight requirements relating to functions carried out under this Agreement. These compliance reviews may include participating in monitoring activities to ensure the timely detection of errors, fraud, waste, and abuse; allowing for certification of performance of agreed-upon procedures; and participating in timely remediation of any findings and recommendations that arise from federal or state audit reviews.

### **3. Consideration and Payment**

- 3.1 All services provided by each agency under this Agreement must be performed to the mutual satisfaction of all parties, as determined at the discretion of each agency's Authorized Representative.
- 3.2 All costs incurred by the Agencies under this Agreement shall be directly charged to appropriate FINDEPT ID according to Exhibits A and B. Direct charges shall only proceed after approval for grant funding has been received by MMB from CCIIO and state approvals under Minn. Stat. § 3.3005 have been obtained.
- 3.3 Modifications to Exhibits A and B may be made by mutual agreement of the workgroup identified in Section 2.1.3 without revision of this Agreement, but such mutual agreement must be made in writing. Modifications related to travel costs may be made by Barb Juelich, MNsure/Minnesota Insurance Marketplace Chief Financial Officer, in consultation with the affected Agencies without the full workgroup.
- 3.4 With prior approval by Barb Juelich, MNsure/Minnesota Insurance Marketplace Chief Financial Officer, reasonable and necessary travel costs incurred by the Agencies in carrying out the duties outlined in this Agreement may be directly charged by the Agencies to appropriate FINDEPT IDs. Upon approving travel, Barb Juelich will increase budget amounts in appropriate FINDEPT IDs and notify the workgroup identified in Section 2.4.1 of the changes to Exhibits A and B.
- 3.5 Cost incurred under Exhibit A and B prior to execution of this Agreement may be included as part of this Agreement.

### **4. Authorized Representatives**

- 4.1 The MDH Authorized Representative is MDH Assistant Commissioner, Ellen Benavides, 625 Robert Street North, St. Paul, MN 55164-0975, 651-201-3565 or her successor.
- 4.2 The Commerce Authorized Representative is Commerce Deputy Commissioner, Tim Vande Hey, 85 7<sup>th</sup> Place East, Suite 500, St. Paul, MN 55101-2198, 651-297-7030, or his successor.
- 4.3 MMB Authorized Representative is April Todd-Malmlov, MN sure/Minnesota Insurance Marketplace Director, 85 7<sup>th</sup> Place East, Suite 500, St. Paul, MN 55101-2198, 651-296-6588, or her successor.

### **5. Amendments**

- 5.1 Any amendment to this Agreement must be in writing and will not be effective until it has been executed and approved by the same parties who executed and approved the original Agreement,

or their successors in office.

## 6. Liability

6.1 Each party will be responsible for its own acts and behavior and the results thereof.

### 1. STATE ENCUMBRANCE VERIFICATION

Individual certifies that funds have been encumbered as required by Minn. Stat. §§ 16A.15 and 16C.05.

Signed: *Veronica Horvath*

Date: 4/22/13

*Contract - 61408*

### 2. Department of Health

By: *[Signature]*

(With delegated authority)

Title: 4-24-13

Date: ASSISTANT COMMISSIONER

### 2. Department of Commerce

By: *Jim Vander Hey*

(With delegated authority)

Title: Deputy Commissioner

Date: 4/23/13

### 3. Minnesota Management and Budget

By: *Dimi*

(With delegated authority)

Title: CEO

Date: 4/25/13





or their successors in office.

## 6. Liability

6.1 Each party will be responsible for its own acts and behavior and the results thereof.

### 1. STATE ENCUMBRANCE VERIFICATION

Individual certifies that funds have been encumbered as required by Minn. Stat. §§ 16A.15 and 16C.05.

Signed: Jennifer Henstien

Date: 4/22/13

#61408

### 2. Department of Health

By: [Signature]  
(With delegated authority)

Title: ASSISTANT COMMISSIONER

Date: 4/24/13

### 2. Department of Commerce

By: Tim Vander Hey  
(With delegated authority)

Title: Deputy Commissioner

Date: 4/23/13

### 3. Minnesota Management and Budget

By: \_\_\_\_\_  
(With delegated authority)

Title: \_\_\_\_\_

Date: \_\_\_\_\_



**Attachment A - Budget for MDH Work Supported by Health Insurance Exchange Grant**

January 25, 2013

<b>Employee Compensation</b>			<b>September 2012 Grant</b>		<b>January 2013 Grant</b>	
Position	FTE	Ann Salary	Months	Total	Months	Total
QHP - Network Adequacy and Quality Review	12.0	75,010	4	300,040	11	825,110
QHP – IT Maintenance	1.0	98,527	4	32,842	5	41,053
Evaluation - Health Economics Director	0.1	93,380	4	3,113	11	8,560
Evaluation Frame - Health Economics Asst. Dir	0.1	74,642	4	2,488	11	6,842
Evaluation Implem - Health Economics Asst. Dir	0.2	74,642	0	-	12	14,928
Evaluation Frame - Health Economics Analyst	0.4	72,036	4	9,605	11	26,413
Evaluation Implem- Health Economics Analyst	0.6	72,036	0	-	12	43,222
MDH HIX Project Manager	1.0	62,000	0	-	11	56,833
<i>Salary Subtotal</i>				348,088		1,022,961
<i>Fringe at 31.8%</i>				110,692		325,302
<b><i>Employee Compensation Line-Item Total</i></b>				<b>458,780</b>		<b>1,348,263</b>
<b>Contracts</b>						
Evaluation Methodology Analysis				75,000		0
<b><i>Contracts Line-Item Total</i></b>				<b>75,000</b>		-
<b>Supplies and Equipment</b>						
Computers				16,900		-
Supplies				6,800		20,525
Communications/printing/misc				5,440		16,420
<b><i>Supplies and Equipment Line-Item Total</i></b>				<b>29,140</b>		<b>36,945</b>
<b>Indirect</b>						
14% capped indirect, standard MDH methodology				71,809		193,929
<b><i>Indirect Line-Item Total</i></b>				<b>71,809</b>		<b>193,929</b>
<b>Grand Total</b>				<b>634,729</b>		<b>1,579,137</b>



# Attachment B - Budget for Commerce Work Supported by Health Insurance Exchange Grant

February 1, 2013

## Employee Compensation

Position	September 2012 Grant				January 2013 grant	
	FTE	Ann Salary	Months	Est Cost	Months	Total
Commerce Rate Analysis	3.0	\$72,036	4	72,036	11	198,097.8
Commerce - Policy Forms Analysis	3.0	\$72,036	4	72,036	11	198,097.8
Commerce - Policy Review Cooredinator	1.0	\$72,036	4	24,012	11	66,032.6
Commerce SPA Director(prorate)	0.5	\$91,350	4	15,225	11	41,868.8
Commerce Enforcement/Complaint Review	2.0	\$72,390	0	-	3	36,195.2
<b>Salary Subtotal</b>				<b>183,308</b>		<b>540,292</b>
Fringe at 31.8%				58,292		171,813
<b>Employee Compensation Line-Item Total</b>				<b>241,600</b>		<b>712,105</b>

## Contracts

	Est Cost	
Policy Forms Analysis	812,500	
<b>Contracts Line-Item Total</b>	<b>812,500</b>	<b>-</b>

## Supplies and Equipment

	Est Cost	
Computers	9,750	
Supplies	3,750	11063
Rent	6,500	19175
Communications/printing/misc	3,000	8850
<b>Supplies and Equipment Line-Item Total</b>	<b>23,000</b>	<b>39,088</b>

## Indirect

	Est Cost	
14% direct charged salaries and fringe	40,544	105,167
<b>Indirect Line-Item Total</b>	<b>40,544</b>	<b>105,167</b>

<b>Grand Total</b>	<b>1,117,644</b>	<b>856,360</b>
--------------------	------------------	----------------



## STATE OF MINNESOTA DEPARTMENT OF HUMAN SERVICES & MNSURE

### INTERAGENCY AGREEMENT

THIS INTERAGENCY AGREEMENT, and amendments and supplements, is between the State of Minnesota, acting through its Chief Executive Officer of the Minnesota Health Insurance Marketplace (hereinafter "MNSure", and the Commissioner of the Minnesota Department of Human Services (hereinafter "DHS").

#### RECITALS

WHEREAS, MNSure, the state health insurance marketplace as described in Minnesota Statutes, section 62V.03, is empowered to enter into interagency agreements pursuant to Minnesota Statutes, section 471.59, subdivision 10;

WHEREAS, DHS is empowered to enter into interagency agreements pursuant to Minnesota Statutes, section 471.59, subdivision 10;

WHEREAS, MNSure is in need of standard, centralized administrative services to enable administrative efficiency;

WHEREAS, DHS has access to specialized resources capable of providing the administrative services sought by MNSure; and

WHEREAS, DHS represents that it is duly qualified and willing to perform the services set forth in this Agreement.

THEREFORE, the Parties agree as follows:

#### AGREEMENT

##### **1. PARTIES' DUTIES- MNSURE BUSINESS OPERATIONS.**

**1.1 Human Resources.** DHS shall provide human resource services to MNSure in accordance with the duties, responsibilities, and obligations set forth in Exhibit B, which are attached and incorporated into this Agreement.

**A. Scope of Work.** MNSure shall retain ownership and responsibility for its human resource decisions, while DHS shall serve in an advisory capacity and provide transaction and other services. MNSure shall be responsible for paying all costs associated with all independent investigations.

**B. Authorized Representatives.**

- 1.** DHS' authorized representative in regards to human resource services is Connie Jones, Human Resources Director, or her successor.
- 2.** MNSure's authorized representative in regards to human resource services is Dave Rowley, General Counsel, or his successor.

3. Each representative shall have final authority for acceptance of human resource services of the other party and shall have responsibility to ensure that all payments due to the other party with respect to human resource services are made pursuant to the terms of this Agreement

## **1.2 Financial Operations.**

### **A. Scope of Work.**

#### **1. Payroll.** DHS shall:

- a. Process bi-weekly employee payroll for MNSure employees.
- b. Process payroll funding and expense corrections to ensure that all salaries are paid from the correct funding source. Corrections will be processed when received or during the next available open pay period.
- c. Process other needed payroll adjustments, including retroactive wage increases, or changes to claimed sick or vacation.
- d. Print and review payroll reports as required by Minnesota Management and Budget (MMB) policy.
- e. Maintain audit trail for payment documents.
- f. Serve as contact for MNSure employees with questions regarding Direct Deposit.

#### **2. Accounts Payable.** DHS shall:

- a. Issue payments to vendors, contractors, carriers, and agencies based on submission of approved invoices from MNSure. Payments will be submitted by MNSure to DHS' Financial Operations Division (FOD) Accounts Payable email in-box and will be paid by FOD within 48 hours of receipt.
- b. Respond to vendors with questions about payments received.
- c. DHS in consultation with MNSure, will establish blanket encumbrances for certain administrative expenses. This includes but is not limited to Central Mail, office supplies as determined by the parties, Issuance Operations Center, Receipt Center, Post Office Box Rentals, and Phone bills.
- d. Process EIORs for Accounts Payable purchase types for items such as training, registrations, and room rentals.
- e. Process refunds due to previously receipted MNSure payments.



- f. Process expenditure corrections related to cost coding of MNSure expenditures (EBFD, AC1 and ProjID codes) within one week of receiving from MNSure;
- g. Establish vendor numbers in SWIFT for payments when needed.
- h. Process Employee Business Expenses.
- i. Maintain audit trail for encumbrance and payment documents.

**3. SWIFT and SEMA4 Security.** DHS shall:

- a. Establish and maintain SWIFT security clearance of MNSure employees as authorized by MNSure's Chief Financial Officer or designee.
- b. Establish and maintain SEMA4 security clearance of MNSure employees as authorized by MNSure's Chief Financial Officer or designee.
- c. Coordinate and include MNSure in the annual MMB security certification process.
- d. Include MNSure in annual review and update of SWIFT security risk assessment.

**4. SWIFT-ER functionality.** DHS shall:

- a. Provide training and access to SWIFT-ER. SWIFT-ER is a web- based custom DHS/MN.IT application that serves as a front-end to the SWIFT Data Warehouse for standard report purposes.
- b. Maintain underlying SWIFT-ER database tables, report programing, and web-based interface.
- c. Coordinate with MMB and their source "staging" tables to ensure the necessary data is accurate and available to refresh the SWIFT-ER database nightly.
- d. Provide Annual SWIFT-ER and database maintenance, the transition between fiscal years requires extensive annual attention by technical staff.

**5. Navigator Program payments.** DHS shall:

- a. Calculate quarterly Navigator Program payments based on program data provided by MNSure.
- b. Stage the quarterly payments in IWP interface file; validate file against SWIFT vendor file.
- c. Coordinate processing IWP interface file with MN.IT and MMB technical staff. (Note: the IWP file interface is maintained by MN.IT, but DHS pays for this service).

- d. Provide Navigator budget vs actual reporting to MNSure.

**6. Accounts Receivable.** DHS shall:

- a. To the extent permitted by Minnesota Statutes, section 16D.13 and MMB, include MNSure in DHS' waiver from not charging simple interest on debts owed to the state of Minnesota.
- b. Provide general assistance on SWIFT Accounts Receivable and Billing functionality.
- c. Provide back-up to MNSure staff on an as needed basis for SWIFT functions to ensure segregation of duties per SWIFT security risk assessment, including running single action process, approving credit bills, and updating customer demographic information.

**7. Collections.** DHS shall:

- a. Provide general assistance of collection questions.
- b. Coordinate referral of past due receivables to Department of Revenue for collections.

**8. Budget Planning & Cost Allocation.** DHS shall:

- a. Provide assistance with budget planning related to Minnesota Eligibility Technology System (METS) by DHS's Financial Operations Director or designee.
- b. Provide Public Assistance Cost Allocation Plan (PACAP) and Operational Advance Planning Document (OAPD) cost allocation services. Negotiate cost allocation methodology and budget with federal agencies.
- c. Provide COCAS administration and technical support as related to Schedule 90 of the PACAP.
- d. Provide METS accounting and Executive Steering Committee (ESC) reporting by FOD staff to the extent it benefits MNSure.

**9. On-going MNSure Financial Responsibilities.** Apart from DHS' duties and obligations under this Section, MNSure shall perform and remain responsible for the activities described in Exhibit C, On-going Financial Responsibilities, which is attached and incorporated into this Agreement.

**10. Receipt Center.** DHS shall provide standard Receipt Center receipting services for MNSure.

**B. Authorized Representatives.**

- 1. DHS's authorized representative in regards to financial operations is Joe Jarosz, Accounting Operations Manager, or his successor.

2. MNSure's authorized representative in regards to financial operations is Gerald Wood, Accounting Operations Director, or his successor.
3. Each representative shall have final authority for acceptance of payroll and accounts payable services of the other party and shall have responsibility to ensure that all payments due to the other party with respect to payroll and accounts payable services are made pursuant to the terms of this Agreement.

### 1.3 Procurement

**A. Procurement Scope of Work.** DHS shall provide procurement support services to MNSure in accordance with the duties, responsibilities, and obligations set forth below. DHS shall provide training and procedural policies, protocols and updates for all of the services described in this section.

1. **Swift Procurement Transactions.** DHS shall encumber and dispatch various types of purchase orders as requested by MNSure via the Electronic Inter-Office Requisition (EIOR) system. This includes the on-going maintenance of such purchase orders and the year-end closing or certification that is required.
2. **Purchasing Card Administration.** Per the DHS Purchasing Card Policy, DHS shall provide training for current and new cardholders, transaction support and/or dispute resolution, monthly reconciliation of transactions in SWIFT, record management and retention via FileNet, account maintenance and support via contracted purchasing card supplier etc.
3. **EIOR Administrative Services.** DHS shall provide training and administrative support for EIOR as it pertains to MNSure's business protocols. This includes granting user access, functional reporting features based on MNSure requests, proper approval routing, accurate FinDept funding sources, etc.
4. **Agency Buyer Support.** Based on commodity, DHS shall support MNSure in the protocol of the procurement process. This includes posting events, coordinating bid events, and training in DHS business processes (Office Supplies, Multi-Function Devices, and other miscellaneous procurement standards).
5. **Receipts and Delivery.** DHS shall provide receiving, SWIFT receipting and internal building to building delivery of commodities shipped to the 444 Lafayette loading dock. Any items that have been pre-approved for direct shipment to MNSure will be receipted as needed per the DHS procedures on handling packing slips from remote locations. This will include fulfilling the requirement of completing the SWIFT receipt process and subsequent 3-way match on required commodities. The appropriate profiles will be built in SWIFT for any asset related items per the DHS Fixed Asset Policy.
6. **Asset inventory and management.** DHS shall coordinate the inventory and management of MNSure fixed assets. This collaborated effort will be in

accordance with the DHS Fixed Asset Policy and Procedures which will outline the process in accordance to State policy.

7. **MMB/ACFR asset reporting.** DHS shall assist in the ACFR reporting to be submitted and certified by a MNSure representative. DHS will update or adjust ACFR records based on data provided by MNSure and the financials created in SWIFT. This collaborated effort will be in accordance with the DHS Fixed Asset Policy and Procedures which will outline the process in accordance to State policy.

**B. Authorized Representatives.**

1. DHS' authorized representative in regards to procurement services is Mike LaValle, Procurement Supervisor, or his successor.
2. MNSure's authorized representative in regards to procurement services is Katie DeGrio Channing, Legal Director or her successor.
3. Each representative shall have final authority for acceptance of procurement services of the other party and shall have responsibility to ensure that all payments due to the other party with respect to procurement services are made pursuant to the terms of this Agreement

#### 1.4 Contracts

- A. Contracts Scope of Work.** DHS' Contracts unit shall enter Contracts and POs in SWIFT for MNSure and MNSure/DHS related contracts according to MNSure/DHS contract work flow procedures. This includes MNSure administered professional technical contracts authorized within the ESC-approved METS budget that are cost allocated 100% to MNSure.

**B. Authorized Representatives.**

1. DHS' authorized representative in regards to contract services is Song Lyfoung, Director of Contracts, Procurement & Legal Compliance, or her successor.
2. MNSure's authorized representative in regards to procurement services is Katie DeGrio Channing, Legal Director, or her successor.
3. Each representative shall have final authority for acceptance of contract services of the other party and shall have responsibility to ensure that all payments due to the other party with respect to contract services are made pursuant to the terms of this Agreement.

#### 1.5 Background Studies.

- A. Scope of Work.** DHS shall provide background study services to MNSure in accordance with the duties, responsibilities, and obligations set forth below. DHS shall:

1. Provide designated MNSure and Assister Resource Center staff with sufficient user access to the DHS NETStudy or NETStudy 2.0 application to allow for the performance of their job duties.
2. Provide staff resources to input and process all Consumer Assistance Partner background study requests in a timely manner.
3. Conduct a review of criminal records maintained by the Minnesota Bureau of Criminal Apprehension, and compare any discovered convictions against the potentially disqualifying criminal offenses specified under Minnesota Statutes, section 245C.15.
4. Notify MNSure through NETStudy or NETStudy 2.0 of the results of each background study.
5. When the result of the background study is a potential disqualification, send the potentially disqualified background study subject a notice explaining the information reviewed, the conclusion reached, the process for challenging the correctness of the information, the process for requesting an individualized review of the individual's fitness and rehabilitation, and the date by which a request for review must be received.
6. Provide MNSure a copy of the notice described in item 5.
7. With respect to the Consumer Assistance Partner programs, work in partnership with MNSure regarding individualized reviews or appeal requested by a background study subject with potential disqualifying conduct or criminal offenses.
8. After transitioning to NETstudy 2.0, monitor MNSure's previous background study subjects through the "Registry Recheck" process and notify MNSure of matches with the Minnesota OIG Excluded Individuals, the Federal OIG List of Excluded Individuals and Entities, and the Minnesota Nurse Aide Registry.

**B. MNSure Responsibilities.** MNSure shall:

1. Request user access for NETstudy or NETstudy 2.0 for appropriate MNSure and Assister Resource Center staff.
2. Provide designated Assister Resource Center and DHS staff with access to MNSure data for these purposes including financial information, identity verification, and other relevant data.
3. Provide background study subjects with privacy notice from NETStudy or NETStudy 2.0.
4. Obtain a signed consent form the background study subject.

**C. Authorized Representatives.**

1. DHS's authorized representative in regards to background study services is Dawn Davis, Division Director or her successor.
2. MNSure's authorized representative in regards to background study services is Christina Wessel, Senior Director of Partner and Board Relations, or her successor.
3. Each representative shall have final authority for acceptance of background study services of the other party and shall have responsibility to ensure that all payments due to the other party with respect to background study services are made pursuant to the terms of this Agreement.

#### **1.6 Fair Hearing and Appeals.**

- A. Scope of Work.** DHS shall provide fair hearing appeal adjudication services to MNSure as described in Exhibit D, Fair Hearing and Appeal Services, which is attached and incorporated into this Agreement.
- B. Authorized Representatives.**
  1. DHS' authorized representative in regards to fair hearing appeal adjudication services is Steven Collins, Appeals Division Director, or his successor.
  2. MNSure's authorized representative in regards to fair hearing appeal adjudication services is Katie DeGrio Channing, Legal Director, or her successor.
  3. Each representative shall have final authority for acceptance of fair hearing appeal adjudication services of the other party and shall have responsibility to ensure that all payments due to the other party With respect to fair hearing appeal adjudication services are made pursuant to the terms of this Agreement.
- C. Consideration.** Consideration for all fair hearing appeal adjudication services performed by DHS pursuant to this Agreement shall be paid by MNSure based on actual case counts and DHS' standard quarterly cost allocation process for appeals adjudication. Appeal adjudications resulting in a decision only on MNSure eligibility issue(s) listed in Exhibit D will be allocated completely to MNSure. Appeal adjudications resulting in a decision on both MNSure eligibility issue(s) and Medicaid/MinnesotaCare (Basic Health Plan) issue(s) will be allocated 50/50 between MNSure and DHS. Monthly, DHS will provide activity reports that the authorized representatives will examine and reconcile on a quarterly basis. The examination and reconciliation will occur within 90 days of the end of the quarter.

#### **1.7 Issuance Operations Center.**

- A. Scope of Work.** DHS shall provide Standard Issuance Operations Center print and mail services for METS and MNSure's QHP program.
- B. Authorized Representatives.**

1. DHS' authorized representative in regards to issuance operation services is Joe Jarosz, FOD Accounting Operations Director, or his successor.
2. MNSure's authorized representative in regards to issuance operation services is Gerald Wood, Accounting Operations Director, or his successor.
3. Each representative shall have final authority for acceptance of issuance operation services of the other party and shall have responsibility to ensure that all payments due to the other party with respect issuance operation services are made pursuant to the terms of this Agreement

## **2. PARTIES' DUTIES -- MINNESOTA ELIGIBILITY TECHNOLOGY SYSTEM ("METS").**

### **2.1 METS System Operations.**

- A. Scope of Work.** DHS through its MN.IT@DHS shall be the technical lead for METS operations as defined and authorized by the METS Executive Steering Committee, and cost allocated in accordance with federally approved DHS Public Assistance Cost Allocation Plan ("PACAP").
- B. Authorized Representatives.**
  1. DHS' authorized representative in regards to METS System Operations services is Ahna Minge, Chief Financial Officer, or her successor.
  2. MNSure's authorized representative in regards METS System Operations services is Kari Koob, Chief Financial Officer, or her successor.
  3. Each representative shall have final authority for acceptance of METS System Operations services of the other party and shall have responsibility to ensure that all payments due to the other party with respect to METS System Operations services are made pursuant to the terms of this Agreement

### **2.2 METS System Development-QHP.**

- A. Scope of Work.** DHS through MN.IT@DHS shall provide METS System Development-QHP services associated with the implementation and enhancement of MNSure's state-based Health Insurance Exchange as authorized by the METS Executive Steering Committee, and cost allocated in accordance with federally approved DHS PACAP.
- B. Authorized Representatives.**
  1. DHS' authorized representative in regards to METS System Development-QHP services is Ahna Minge, Chief Financial Officer, or her successor.
  2. MNSure's authorized representative in regards to METS System Development-QHP services is Kari Koob, Chief Financial Officer, or her successor.
  3. Each representative shall have final authority for acceptance of METS System Development-QHP services of the other party and shall have responsibility to

ensure that all payments due to the other party with respect to METS System Development-QHP services are made pursuant to the terms of this Agreement.

### **3. Occupancy and IT Support Indirect Costs.**

**3.1 Scope of Work.** Payments made and invoices submitted between DHS and MNSure under Section 1 and Section 2.1 of this Agreement are based on direct costs, including the associated Full Time Employee (FTE) positions. This Section addresses the occupancy and IT support indirect costs attributable to these FTE positions. DHS may submit, and MNSure shall pay, invoices for occupancy and IT support indirect costs associated with FTE assigned to perform work under this Agreement.

#### **3.2 Authorized Representatives.**

1. DHS' authorized representative in regards to occupancy and IT support indirect costs is Marty Cammack, Financial Operations Director, or his successor.
2. MNSure's authorized representative in regards to occupancy and IT support indirect costs is Kari Koob, Chief Financial Officer, or her successor.
3. Each representative shall have final authority for acceptance of IT support services of the other party and shall have responsibility to ensure that all payments due to the other party with respect to IT support services are made pursuant to the terms of this Agreement

### **4. DHS PUBLIC HEALTH CARE PROGRAMS.**

**A. Scope.** DHS and MNSure acknowledge that under an Interagency Agreement titled "Interagency Services Agreement for MNSure Participation In the Administration of the Minnesota State Plan or Services Under Title XIX" and dated November 3rd, 2014, which is incorporated into this Agreement by reference, each party has separate and independent obligations related to MNSure's role in DHS' public health care programs.

1. Under the above referenced Interagency Agreement, MNSure has a separate obligation to provide enrollment activities, including eligibility determination, case management, policy renewal, outreach, and post-eligibility activities to DHS for Minnesotans seeking benefits under DHS's public health care programs, including Medical Assistance and MinnesotaCare.
2. The Parties acknowledge that services provided by MNSure under the above referenced Interagency Agreement benefit DHS' public health care programs.
3. DHS' and MNSure's roles and responsibilities in the operation, support, and implementation of the Consumer Assistance Programs, including the Navigator Program and Certified Application Counselor Program, and the Assistor Resource Center shall be governed by Exhibit E, Consumer Assistance Program, which is attached and incorporated into this Agreement.



- B. Estimated Payments.** Under the above referenced Interagency Agreement, the Parties acknowledge that DHS has a separate and independent obligation to pay MNSure for MNSure administrative costs attributable to the DHS' public health care programs according to the DHS Public Assistance Cost Allocation Plan ("PACAP"). The estimated amounts are as follows:

1. SFY2022: \$13,280,000
2. SFY2023: \$13,550,000

The amounts specified in this Section are estimates only. This Agreement does not obligate DHS to pay MNSure the amounts estimated in this Section for any service performed in this Agreement or the Interagency Agreement referenced in Paragraph 1 of this Section, but it does obligate DHS to pay for actual costs as described in the interagency agreement specific to the PACAP.

## **5. CONSIDERATION AND TERMS OF PAYMENT.**

### **A. Payment Structure.**

1. **Section 1 Parties' Duties - MNSure Business Operations.** Consideration for all services performed by DHS under Section 1 of this Agreement represents MNSure's payment to DHS for DHS administrative and business operations costs attributable to MNSure's private health care programs.
2. **Section 2 Parties' Duties - METS Services.** Consideration for all services performed by DHS under Section 2 of this Agreement represents MNSure's payment to DHS for METS system operation and development costs attributable to MNSure's private health care programs,
3. **Section 3 Occupancy and IT Support Indirect Costs.** Payments made and invoices submitted between DHS and MNSure under Section 1 and Section 2 of this Agreement are based on direct costs, including the associated FTE allocation. Compensation under Section 3 represents the occupancy and IT support indirect costs attributable to these FTE positions.
4. **Payment Methodology.** Payments made and invoices submitted between DHS and MNSure shall be in accordance with the DHS Public Assistance Cost Allocation Plan ("PACAP") methodology and associated Central Office Cost Allocation System ("COCAS") policies and procedures, and in accordance with Centers for Medicare & Medicaid Services' ("CMS") advance planning documents ("APDs") associated with Minnesota's Medicaid Eligibility Determination System ("MEDs"), which are hereby incorporated into this Agreement by reference.

- B. Consideration.** Consideration for all services performed by DHS pursuant to this Agreement shall be paid by MNSure in accordance with the allocations set forth in Exhibit A, Budget, as amended, which is attached and incorporated into this Agreement.

- C. Terms of Payment.** Payment shall be made by MNSure on a quarterly basis within thirty (30) days after DHS has presented Invoices for services performed to MNSure. DHS shall present invoices to MNSure within forty five (45) days after each calendar quarter end.
- D. Total Obligation.**
1. **MNSure Business Operations Services.** The total obligation of MNSure for all compensation and reimbursements to DHS for non-IT related services under this Agreement shall not exceed **two million two hundred and five thousand dollars (\$2,205,000)**, unless otherwise stated in Exhibit A, Budget as amended.
  2. **METS Services.** The total obligation of MNSure for all compensation and reimbursements to DHS for IT related services under this Agreement shall not exceed **ten million five hundred and eighteen thousand and two hundred fifty-nine dollars (\$10,518,259)**, unless otherwise stated in Exhibit A Budget, as amended.
  3. **Occupancy and IT Support Indirect Costs.** The total obligation of MNSure for all compensation and reimbursements to DHS for occupancy and IT support indirect costs under this Agreement shall not exceed **three hundred and fifty thousand dollars (\$350,000.00)**, unless otherwise stated in Exhibit A, Budget as amended.
- E. Advance Payments.** MNSure's and DHS's Chief Financial Officers, or their successors, may, based on estimated, invoices, authorize advance payments between MNSure and DHS for the limited purpose of addressing cash flow issues resulting from quarterly PACAP and COCAS procedures. Advance payments made under this Section must be settled against the next invoice and shall not exceed line item amounts set forth in Exhibit A, Budget.
- F. Section 4 DHS Public Health Care Programs.** Section 4 of this Agreement represents DHS' separate and independent obligation to pay MNSure for MNSure administrative costs attributable to the DHS' public health care programs. This Agreement does not obligate DHS to pay MNSure the amounts estimated in Section 4 for any service performed in this Agreement or the Interagency Agreement referenced in Section 4.
- 6. CONDITIONS OF PAYMENT.** All services provided by DHS pursuant to this Agreement shall be performed to the satisfaction of MNSure, as determined at the sole discretion of its Authorized Representative.
- 7. TERMS OF AGREEMENT.** This Agreement shall be effective on **October 1, 2021** without regard to the Execution Date of this Agreement, and shall remain in effect through **June 30, 2023**, or until all obligations set forth in this Agreement have been satisfactorily fulfilled, whichever occurs first. Upon the Execution Date of this Agreement, all previous agreements between DHS and MNSure for goods and services , covered by this Agreement shall terminate and be replaced by this Agreement. All previous agreements between DHS and MNSure for goods and services not covered by this Agreement shall remain in full force and effect.

8. **CANCELLATION.** This Agreement may be canceled by MNSure or DHS at any time, with or without cause, upon thirty (30) days written notice to the other party. In the event of such a cancellation, DHS shall be entitled to payment, determined on a pro rata basis, for work or services satisfactorily performed.
9. **ASSIGNMENT.** Neither DHS nor MNSure shall assign or transfer any rights or obligations under this Agreement without the prior written consent of the other party.
10. **AMENDMENTS.** Any amendments to this Agreement shall be in writing, and shall not be effective until executed by the same parties who executed the original agreement, or their successors in office.
- A. In the event of an emergency, MNSure's and DHS's Chief Financial Officers, or their successors, may agree, in writing, to the provision and payment of services not otherwise addressed in this Agreement. For purposes of this Section, an emergency shall have the same meaning as Minnesota Statutes, section 16C.02, subdivision 6(b) and due to time constraints, cannot be addressed with an immediate amendment to this Agreement. All services and payments authorized under this Section must be incorporated into a formal amendment in accordance with Section 8 above within a reasonable time after the emergency.
11. **LIABILITY.** DHS and MNSure agree that each party will be responsible for its own acts and the results thereof to the extent authorized by law and shall not be responsible for the acts of the other and the results thereof. The DHS and the MNSure liability shall be governed by the provisions of the Minnesota Tort Claims Act, Minnesota Statutes, section 3.736, and other applicable law.
12. **INFORMATION PRIVACY AND SECURITY.** Information privacy and security shall be governed by the "Data Sharing Agreement and Business Associate Agreement Terms and Conditions", identified as DSK 187696, as amended, or the applicable successive Data Sharing Agreement executed by the Parties, which is incorporated into this Agreement by reference. DHS and MNSure respectively agree that each party shall fully comply with the terms of the Data Sharing Agreement when carrying out any duties or obligation identified in this Agreement.

**Remainder of Page Intentionally Left Blank  
(Signature Page Follows)**

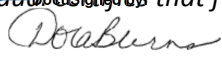
Contract No. IAK \_201592\_\_\_\_\_

IN WITNESS WHEREOF, the parties have caused this Interagency Agreement to be duly executed  
intending to be bound thereby

APPROVED:

### 1. REQUESTING AGENCY ENCUMBRANCE VERIFICATION

*Individual certifies that funds have been encumbered as required by Minn. Stat. §§ 16A.15 and 16C.05*

By:   
5457B11AE8BB49D...

Date: 9/30/2021

SWIFT Contract No: IAK 201592

SWIFT PO #: 3-1823

### 2. MN Department of Human Services


By:   
F336517A7B0D41E...

*With delegated authority*

Title: Deputy Commissioner

Date: 10/13/2021

### 3. MNSure

By:   
F3466CF591CC40D...

*With delegated authority*

Title: CFO

Date: 10/14/2021

Distribution:

Requesting Agency – Original (fully executed) contract

Providing Agency

Contracting & Legal Compliance, Contracts Unit- #0238

**EXHIBIT A – Interagency Agreement Budget**

Section (i.e. services to be provided)	Basis for	Authorized Representative		Totals	
	Amount Charged	MNsure / Kari Koob	DHS / Ahna Minge or successor	2 <sup>nd</sup> -4 <sup>th</sup> quarters FY2022	FY2023
1.1 Human Resources	Fixed	Dave Rowley	Connie Jones	150,000	200,000
1.2 Financial Operations	Fixed	Gerald Wood	Joe Jarosz	112,500	150,000
1.3 Procurement	Fixed	Katie DeGrio Channing	Mike LaValle	63,750	85,000
1.4 Contracts	Fixed	Katie DeGrio Channing	Song Lyfoung	11,250	15,000
1.5 Background Studies	Variable	Christina Wessel	Dawn Davis	18,750	25,000
1.6 Fair Hearing and Appeals	Variable	Katie DeGrio Channing	Steven Collins	375,000	500,000
1.7 Issuance Operations Center	Variable	Gerald Wood	Joe Jarosz	213,750	285,000
<b>Total Business Operation Services</b>				<b>945,000</b>	<b>1,260,000</b>
2.1 METS System Operations	Variable	Kari Koob	Ahna Minge or successor	4,620,087	5,898,172
2.2 METS System Development-QHP	Variable	Kari Koob	Ahna Minge or successor	0	0
<b>Total METS Services</b>				<b>4,620,087</b>	<b>5,898,172</b>
<b>3. Occupancy and IT Support Indirect Costs</b>	Fixed	Kari Koob	Marty Cammack	<b>150,000</b>	<b>200,000</b>
<b>Total Interagency Agreement</b>				<b>5,715,087</b>	<b>7,358,172</b>
					13,073,259

**EXHIBIT B - Human Resource Services**

DHS will provide the agency the following human resource services that will help MNsure operate effectively:

**Transactions**

- Complete accurate and timely SEMA-4 changes related to changes in employee information, hire, funding; promotion, separation dates, increase dates, department ID, medical leaves of absence, performance reviews, etc.
- Seniority Rosters will be updated/posted as required by contracts/plans.

Timely transactions depend on DHS receiving timely information from MNsure about employee status. DHS is not responsible for processing information if it has not received a written request.

***Performance Management***

Definition: Developing standards and policies and providing support for supervisors and managers to provide constructive and developmental feedback and direction for 'ongoing coaching as well as a context for management decision-making.

- Train management on performance improvement techniques.
- Advise managers and supervisors in investigating employee misconduct, performance or attendance problems, or recommend retention of an outside Investigator. Investigations for managerial staff will be referred to an independent Investigator outside the state. DHS will coordinate the investigation.
- Advise managers and supervisors on handling performance, attendance, and conduct issues with employees.
- Assist managers and supervisors in withholding performance increases, taking disciplinary action, or discharging employees.
- Draft disciplinary letters and letters of expectations.
- Advise managers and supervisors on human resources best practices in employee motivation, reviews, and supervisory practices.

MNsure is responsible for paying all costs associated with independent investigations.

***Human Resources Policy Management***

Definition: Researching, developing, recommending, implementing, and communicating an array of Human Resources policies to support consistent employment practices.

- Investigate the need for and write new policies for human resource issues.
- Maintain and update existing policies.

**Contract Administration**

- Advise managers and supervisors on the proper application of contract language. When appropriate, DHS will seek MMB's advice on contract interpretation.
- Advise managers and supervisors on the practical application of employment laws such as FMLA, FLSA, ADA, USERRA, and all discrimination laws.

***Training***

Definition: Providing strategy, planning, and implementation of targeted learning activities to support both individual employee development and organizational strategies. This training is restricted to employees of MNsure.

- In conjunction with MNsure HR Specialist, train managers and supervisors on human resources practices, employment law, bargaining unit contract language/ compensation, code of ethics, and other topics directly related to human resources.

***Classification and Compensation***

Definition: Conduct an analysis of the individual position to identify and describe the different kinds of work in an organization and group similar positions under common classification titles based upon the kind of work, degree of difficulty and the, responsibilities required.

- Review position descriptions; determine appropriate classification, document audit decisions, and explain the rationale for classification decisions.
- Coordinate Hay sessions when applicable.
- Conduct studies of groups of positions as necessary.
- Approve or deny compensation requests for new hires or promotions.
- Supervisors will receive notification of positions that are ending each quarter.

MNsure must provide documentation of requests to convert unclassified position to the classified service at least one month in advance of the end of the unclassified position.

DHS has received delegated authority from MMB-Enterprise Human Resources to make classification and compensation decisions. DHS must abide by accepted practices and rules governing classification and compensation in order to retain this delegation. MMB-Enterprise Human Resources periodically audits DHS's work to determine compliance with rules and laws.

***Vacancy-Filling***

Definition: Work With HR Specialist who works directly to assist managers in hiring so that MNsure follows state bargaining unit contracts, employment laws, and state laws governing state positions. This includes filling vacancies by developing appropriate qualifications for vacancies<sup>1</sup> determining recruitment options, posting, reviewing candidates re<sup>1</sup>umes to determine qualified candidates, and assisting the supervisor or managers in following state bargaining unit contracts and state laws.

- Advise on minimum qualifications and recruitment options.
- Posting and bidding/expression of interest process for classified positions.
- Review position applications to determine which applicants meet the minimum qualifications and refer successful candidates to the hiring supervisor.
- Assist managers and supervisors in developing interview questions and other selection criteria and exercises.
- Conduct background checks.
- Document hires for affirmative action purposes.
- Compose offer and employment confirmation letters.
- Notify all applicants of position hiring decisions.
- Close out Resumix

***Labor Relations and Employment Law***

Definition: Ongoing maintenance and development of union and employee relations in order to advise management on performance and employment law issues, standards; and policies.

- Represent management at meet and confer sessions.
- Respond to third-step grievances for MNSure.
- Review and responding to requests for accommodation under the ADA.
- Monitor payroll and leave under USERRA.
- Notify MNSure of new laws, state rules, and issues.
- Investigate all significant workers' compensation claims, process claims, and work through settlements and resolutions on behalf of MNSure.
- Advise supervisors and managers with other employment law issues such as discrimination, sexual harassment, etc.
- Review unemployment claims and represent management in unemployment hearings.

***Safety & Workers' Compensation***

- File yearly OSHA lost-time reports.
- Assist with first reports of injury filings.

***Reporting***

- Upon request, provide ad hoc reports on employee costs, leave use, hires, separations, and other employment Information contained in the state's information warehouse.

***File Maintenance & Storage***



- Maintain and store audit (Job classification decision) files and requisitions (vacancy filling) files.
- Inform MNSure on the types of personnel information that should be securely maintained onsite.
- Maintain Personnel files/records.

**DHS Human Resources Responsibilities:**

DHS will provide the following level of service:

- Vacancies will be posted within two business days of receipt of a request to fill (if the position does not need to be allocated or the allocation changed)
- Examine 1-9 documentation, after hire, for legal hiring.
- Positions requiring initial allocation will be allocated within two weeks of the receipt of a complete position description, organizational chart, and request memo.
- Positions requiring reallocation will be audited within four to six weeks of the receipt of a complete position description, organizational chart, and request memo.
- Investigations will be conducted promptly. Timing depends on the exact circumstances and availability of union representatives.
- Transactions turned in by Thursday of the non-payroll week will take effect that payroll period.
- Employees hired during the last two days of the pay period may not be paid for those days until the next pay period.

**MNSure's Responsibilities:**

Management of MNSure is responsible for the actions of the organization's employees, including unethical, violent, or harassing behavior and failure to follow state policies and procedures.

MNSure is responsible for completing the following human resource actions:

***Benefits Administration***

- Convey benefits information from Minnesota Management and Budget (DHS) to employees of MNSure.
- Benefits questions and issues will be handled directly by the State Employee Group Insurance Program (SEGIP) at MMB. All employees will receive information on the SEGIP contact.
- FMLA requests: All employees will receive information on how to apply for FMLA from DHS and supervisors and managers will coordinate directly with DHS.

***Training***

Definition: Providing strategy, planning, and Implementation of targeted learning activities to support both individual employee development and organizational strategies. This training is restricted to employees of MNSure.

- In conjunction with DHS, train managers and supervisors on human resources practices, employment law, bargaining unit contract language, compensation, code of ethics, and other topics directly related to human resources.

- Track completion on topics mandated by law or policy - code of conduct, sexual harassment prevention, right-to-know, etc.
- Send communications to employees about various human resource topics.

***Policies and Procedures***

- MNsure has appointed an Ethics Officer and communicated that designation to employees.
- Employees are trained on the Code of Ethics (M.S. 43A.18) and as required the Code of Conduct.
- Position descriptions clearly indicate the employee's level of decision-making authority.
- Employees receive copies of general statewide policies and policies and procedures governing their particular jobs.
- Formal delegations of duties are on file.
- Operating practices are consistent with state policies.
- Appropriate action is taken for violations of policy.

***Position Descriptions***

- All positions have position descriptions that are updated at least every three years.
- Position descriptions are consistent with employees' actual job duties and include a listing of essential functions under the ADA.

***Employee Performance Management***

- New employees must receive copies of their position descriptions and an orientation to their work and their work unit,
- All new employees must receive mid-probationary and probationary reviews.
- All employees must be given honest feedback on their performance at least once a year with a written formal evaluation placed in their personnel
- Performance expectations are made clear for all employees.
- Employees whose performance, attendance, or behavior is problematic will be coached on their deficiencies to permit them to Improve- unless the behavior is so severe that immediate action must be taken to end their appointment. All such issues should be discussed with the DHS Labor Relations Representative.

**EXHIBIT C - On-going MNSure Financial Responsibilities**

Apart from DHS' duties and obligations under Clauses 1.2 "Financial Operations", 1.3 "Procurement" and 1.4 "Contracts" of this Agreement, MNSure shall perform and remain responsible for the following activities:

1. Management of overall MNSure finances and operating budget with the federal government, Minnesota Management and Budget (MMB) and the MNSure Board of Directors.
2. Reconciliation of MNSure-related legislative actions to MMB Fund Balance Statements; reconciliation of MNSure Enterprise Fund activity to MMB Financial Statements (ACFR).
3. Administration of federal grant applications and awards, including coordination with DHS federal APD projects and associated MNSure/DHS cost sharing.
4. Administration of federal fiscal reporting requirements; responses to data requests from federal agencies and /or auditors.
5. Management of SWIFT Agency H60 (MNSure) chart of accounts, budget structure, and budget/commitment control.
6. Coordination with MMB Executive Budget Officer (s) assigned to MNSure; authorization of SWIFT Agency H60 (MNSure) appropriation transfers and cash flow assistance.
7. Forecasting MNSure premium withhold revenue; budgeting and accounting for premium withhold revenue, including invoicing process.
8. Accounting for and reconciliation of MNSure premium pass-through activity within SWIFT and with the MNSure System (as applicable).
9. Contract management, including legal/attorney function including drafting and review and SWIFT processes (professional technical contracts and grant contracts)
10. Ensuring timely, policy compliant, SEMA4 Employee Self-Service Timesheet completion and supervisory approvals; and associated employee Business Expense approvals.
11. Ensuring MNSure's SEMA4 Department ID structure and SEMA4 position funding records are maintained consistent with the current organization structure and available funding.
12. Initiation and approval of E-1768 personnel transaction, including completion of the Funding Tab when required.
13. Initiation and approval of EIOR commodity purchases, including the Fund Approver role.
14. Approval of special expenses requests and employee business expenses (e.g. travel).
15. Approval of vendor/interagency invoices for payment; timely delivery of approved invoices to DHS Accounts Payable.
16. Maintaining SWIFT customer file so invoicing processes are timely.

17. Troubleshooting and direct follow-up with vendors and customers on payment/invoice inquiries and issues.
18. Annual certifications to MMB, for example: annual spending plan, accounts receivable, financial statement accruals, encumbrances at fiscal year close, ACFR, federal Single Audit Schedules, etc.
19. Updating of Biennial Budget System (a.k.a BPAS), including budget maintenance, narratives and fiscal pages.
20. Coordination of MNsure technology system related fiscal notes/assumptions with ~~DH\$~~ DHS Budget Analysis Division.
21. Administration of interagency agreements with DHS.

## EXHIBIT D - Fair Hearing and Appeal Services

### 1. DHS Duties. DHS shall:

- A. Maintain adequate staffing levels for services specified in this Exhibit by employing: human services judges, paralegals, administrative support staff, and supervisor human services judges.
- B. Adjudicate, including issuing final orders of eligibility determinations, certain specified MNsure eligibility appeals, as agreed upon by DHS and MNsure, including carrier eligibility determination review appeals.<sup>1</sup>
- C. Manage the intake of certain specified MNsure eligibility appeals, as agreed upon by DHS and MNsure.
- D. Provide a representative sample of redacted final decisions to be publicly posted.
- E. Send all correspondence regarding MNsure eligibility appeals to the parties, including, but not limited to, an acknowledgement of receipt of appeal requests and hearing notices.
- F. Submit measurable reports, as agreed upon, to MNsure.
- G. Investigate and respond to all complaints received pertaining to DHS's handling of MNsure appeals, copying MNsure's Authorized Representative.

### 2. MNsure Duties. MNsure Shall:

- A. Provide the consultation, coordination, and directive services of a full time MNsure Appeals Manager.
- B. Provide the design for public interfacing for MNsure eligibility appeals.
- C. Pay DHS in accordance with Clause 1.6 of the Interagency Agreement and attached Budget.
- D. Provide appeal summaries to DHS in accordance with the timelines and other requirements of Minnesota Rules, part 7700.0105, subpart 10, and other applicable law.

### 3. DHS Tasks.

- A. **Staffing and Training.** DHS will provide sufficient staffing levels necessary for adjudicating eligibility appeals and all other functions incorporated through this Agreement, in accordance with state and federal law and MNsure policies and

---

<sup>1</sup> 1 Carrier eligibility determination review appeals are in accordance with section 2.3 of the MNsure Carrier Business Agreement, whereby a carrier offering plans through MNsure may request a formal review of an eligibility determination or redetermination made by MNsure with respect to an enrollee of the Carrier.

procedures: DHS will monitor staffing levels on an ongoing basis and will preemptively identify options for filling staffing vacancies on short notice. DHS will monitor on an ongoing basis all staffing and training weakness and report the same upon identification to MNSure, which will actively identify potential solutions for DHS to explore.

B. **Adjudication.** DHS will adjudicate certain specified MNSure eligibility appeals as agreed upon by DHS and MNSure on:

1. Any MNSure determination of eligibility to enroll in a Qualified Health Plan (QHP) through MNSure, including redeterminations in accordance with 45 C.F.R. § 155.305 (a)- (b); 45 C.F.R. § 155.330; and 45 C.F.R. § 155.335;
2. Any MNSure determination of eligibility for and level of Advance Premium Tax Credit (APTC), and eligibility for and level of Cost Sharing Reductions (CSR), including redeterminations in accordance with 45 C.F.R. § 155.305 (f)-(g); 45 C.F.R. § 155.330; and 45 C.F.R. § 155.335;
3. Any MNSure determination or redetermination of eligibility for employee and/or employer in a Small Business Health Option Program (SHOP) in accordance with 45 C.F.R. § 155.710 (a) and 45 C.F.R. § 155.710 (e);
4. Any failure by MNSure to provide timely notice of an eligibility determination in accordance with 45 C.F.R. § 155.310 (g), 45 C.F.R. § 155.330 (e)(i)(ii), 45 C.F.R. § 155.335 (h)(ii), 45 C.F.R. § 155.610 (i) or 45 C.F.R. § 155.715 (e)-(f); and
5. Any MNSure determination of start date or termination of Exchange enrollment or coverage pursuant to 45 C.F.R. § 155.430; and
6. In response to a notice sent by MNSure under 45 C.F.R. § 155.310 (h), a determination that an employer does not provide minimum essential coverage through an employer- sponsored plan or that the employer does provide coverage but is not affordable coverage with respect to an employee.
7. Carrier eligibility determination review appeals, in accordance with section 2.3 of the MNSure Carrier Business Agreement, whereby a carrier offering plans through MNSure may request a formal review of an eligibility determination or redetermination made by MNSure with respect to an enrollee of the Carrier.

The adjudication of MNSure appeals will offer all procedural due process required by federal and state law; offer all accessibility rights under state and federal law; and will adhere to all final and proposed state and federal regulations governing the adjudication of MNSure appeals. The adjudication will honor the timelines specified in state and federal law. The adjudication includes "expedited appeals," in accordance with 45 Code of Federal Regulations, part 155.540, and MNSure policies and procedures. The adjudication will include, but not be limited to, the following components:

- a. A written recommended decision;
- b. A telephone hearing, a videoconference hearing, or an in-person hearing, when required;
- c. A prehearing conference, if deemed necessary by the presiding judge;
- d. A notice and order for hearing

- e. A MNSure Order issued on behalf of the MNSure Board;
- f. Digital recording of the hearing;
- g. Language Interpretation and translation services, where requested, provided, assistance from MNSure in exploring options for providing in-person interpretation when requested; and
- h. Compliance with all MNSure policies and procedures related to appeal adjudication.

**C. Intake and Finalization.**

- 1. DHS will provide, at minimum, daily monitoring of the designated EDMS folder to check any eligibility records to transfer from MNSure to DHS. DHS will input all received MNSure appeals forms into the case management system (CMS), categorize and assign the appeals. MNSure reserves the right to review appeal requests and informally resolve them internally.
- 2. DHS will input the eligibility records received from MNSure and/or received directly from the appellant into the CMS or records management system (EDMS). DHS is responsible for ensuring accumulation of the appeal record, until a final order is issued and the entire Appeal record is uploaded to EDMS and comprehensive appeal record retention, including the digital recording of the hearing.
- 3. Upon final order, DHS will input the entire Appeal record into the designated EDMS folder for MNSure to maintain. MNSure is the official record holder for the official appeal record once final and uploaded to EDMS.

- D. Redaction.** DHS shall redact for public viewing a sizeable representative sample of MNSure Orders in accordance with state and federal data privacy laws. The size of the representative sample and the methodology for the sampling will be agreed upon by the parties.

DHS will carefully review each Order chosen for redaction so as to redact all identifying information on a case-by-case basis, in addition to redacting all standard identifiers. DHS will upload each redacted order to the decisions database designated by MNSure.

**E. Sending and Maintaining Correspondence.**

- 1. Upon request, DHS will send all correspondence regarding filed MNSure appeals, including, but not limited to, an acknowledgement of receipt of appeal requests, hearing notices, decisions and MNSure Orders, and reconsideration requests to MNSure.
- 2. All correspondence related to MNSure appeals will use letterhead approved by MNSure's Authorized Representative, and will use the appropriate MNSure appeals correspondence template.
- 3. Correspondence that must be mailed in a "timely" manner will be sent on or before 10 (ten) business days. Final Orders will be mailed within 1 (one) business day of finalization and within 90 (ninety) days of receipt of request, as administratively feasible. Dismissals of expedited appeals and final Orders of expedited appeals will be sent within the timeframes as determined by the Secretary of the United States Department of Health and Human Services.
- 4. A copy of all MNSure appeals correspondence will be retained in the case management system, as part of the appeal record. All correspondence related to MNSure appeals will be post-marked

no later than one calendar day following the date listed on the MNsure appeals correspondence (i.e., all MNsure appeals correspondence post-marked on Monday will reflect Monday's date on the letter).

5. DHS will investigate all returned MNsure appeals correspondence, and notify MNsure's Authorized Representative of all returned MNsure appeals correspondence and their respective resolutions on a weekly basis.
- F. **Reporting.** DHS shall submit to MNsure's Authorized Representative reports to measure various metrics pertaining to MNsure appeals, including, but not limited to, number of appeals; number of hearings; timeliness of pending appeals; timeliness of finalized appeals; caseloads; requests for reconsideration, and any metrics measured by state and/or federal reporting needs or audits. The frequency of these reports will be as agreed upon by MNsure's Authorized Representative and DHS' Authorized Representative and will include both regularly reoccurring reports and reports in response to ad hoc requests.
- G. **Investigation and Response to complaints.** DHS will investigate and respond to all complaints received pertaining to DHS's handling of MNsure appeals and respond to complainant, copying MNsure's Authorized Representative, within 30 days of receiving complaint, per the policy and procedure developed according to this Statement.
- H. **Invoicing.** DHS will submit to MNsure's Authorized Representative, quarterly itemized invoices unless otherwise stated in this Agreement.
4. **MNsure Tasks.**
  - A. **Consultation, Coordination, and Direction.** MNsure shall employ and provide a full-time MNsure Appeals Manager to consult, coordinate, and direct services under this Exhibit D. The MNsure Appeals Manager will coordinate the efforts of the parties under this Agreement; organize as needed meetings; serve as a subject matter expert for MNsure appeals; and generally be available to consult and provide direction on a need-be basis for DHS. In the absence of the MNsure Appeals Manager (e.g., vacation), an interim replacement will be identified.
  - B. **Public Interfacing for MNsure appeals.** MNsure will provide the sole public interfacing for MNsure appeals by making appeal information and materials available on its website and through outreach plans developed by MNsure.
  - C. **Payment.** MNsure will pay DHS upon acceptance by MNsure that the tasks and deliverables have been completed, and in accordance with the invoices of each respective agency and the costs as detailed above,
  - D. **Appeals Summaries.** MNsure will provide DHS appeal summaries in accordance with the timelines and other requirements of Minnesota Rules, part 7700.0105, subpart 10, and other applicable law.



**Exhibit E - Consumer Assistance Program**

1. **MNsure's Responsibilities.** MNsure will operate the Consumer Assistance Programs, including the Navigator Program, Certified Application Counselor program, and the Assister Resource Center ("ARC"). Operational responsibilities include:
  - A. **Contracting.** MNsure will:
    1. Process all consumer assistance partner applications and contracts;
    2. Specifically identify DHS as a third-party beneficiary in all Consumer Assistance Partner contracts including, Certified Application Counselor Services Agreements, and Joint Powers and Grant Navigator/In-Person Assister Agreements.
    3. Request input from DHS's Contracts division on the creation and modification of all consumer assistance partner contract templates.
  - B. **Training, resource pages and manual.** MNsure will:
    1. Develop, implement, and maintain certification and recertification training for all consumer assistance partners
    2. Request input and content from DHS' Health Care Administration on all consumer assistance partner training related to public programs.
    3. Update and maintain the navigator resource webpages.
  - C. **Certification.** MNsure will:
    1. Process all consumer assistance partner certification, recertification, and decertification.
    2. Resolve all complaints against consumer assistance partners.
  - D. **Customer Service and Support.** MNsure will:
    1. Provide customer services and support to consumer assistance partners through the ARC.
    2. Oversee supervision, hiring, work direction and priority setting as it relates to staffing and work activities of the ARC.
    3. Develop, implement, and maintain operational support for all consumer assistance partners.
    4. Obtain input and approval from DHS Health Care Administration on all consumer assistance partner communications related to public programs.
  - E. **Compensation.** MNsure will:
    1. Seek approval from DHS FOD for all consumer assistance partner payments and provide necessary data.

2. Request input from DHS on all consumer assistance partner compensation model decisions.
3. Maintain all consumer assistance partners' compensation according set forth in the Consumer Assistance Partner contracts, and not make any modifications to Consumer Assistance Partner compensation rates without the explicit approval of DHS.
4. Implement controls to ensure Consumer Assistance Partner compensation payments are appropriate and audit as needed to safeguard against potential fraud or misuse.
5. Consistent with Clause 1.5 (Internal Audits) of this Agreement, cooperate with DHS audits of consumer assistance partner payments. In the event of an audit of Consumer Assistance Partner payments initiated by MNSure that requires cooperation and assistance from DHS, MNSure shall provide reasonable notice of such an audit. MNSure will work with DHS to avoid disruption of DHS business operations during audit.
6. Be responsible for working with MN.IT staff to develop payment reports, clean data, run report, and develop and send payment statements.
7. Respond to all questions about and facilitate resolving issues regarding compensation.

**2. DHS' Responsibilities.** DHS will support the operations of consumer assistance programs, including the Navigator program and Certified Application Counselor program. Support responsibilities include:

**A. Contracting.** DHS will:

1. Participate as third-party beneficiary to all consumer assistance partner contracts with MNSure, including Certified Application Counselor Services Agreements, and Joint Powers and Grant Navigator/In-Person Assister Agreements.
2. Provide input from DHS Contracts division on all consumer assistance partner contract templates.
3. Provide review on all requested changes to templates.
4. DHS Contact: Song Lyfoung, Director, Contracts, Procurement, and Legal Compliance, 444 Lafayette Road, St. Paul, MN, or her successor.

**B. Training, Resource Pages and Manual.** DHS will:

1. Provide reviewers for training content developed by MNSure. This review will occur on a mutually agreed-upon schedule.
2. Review public program related processes within the navigator manual and navigator resource webpages on a mutually-agreed upon schedule.

3. DHS Contact: Christina Cox; Supervisor, Training and Partner Relations, HCEO, 540 Cedar Avenue, St. Paul, MN, or her successor.

**C. Customer Service and Support.** DHS will:

1. Respond to public program policy questions from the ARC within ten working days through the DHS' HCEO County Relations Resource Center.
2. Provide timely input and approval from DHS HCEO on all consumer assistance partner communications related to public programs,
3. Provide Assister Resource Center (ARC) staff and the ARC supervisor with access to SIR, MMIS; MAXIS and DHS FileNet upon request to provide consumer assistance partner support for public programs per appropriate law and policy.
4. Designate a point person and backup for ARC questions that are more time sensitive for the County Relations Resource Center. These staff will be available during regular DHS business hours (8am-4:30pm),
5. DHS Contact: Isaac Akpojotor, Supervisor, Resource Center Systems Support, HCEO, 540 Cedar Avenue, St. Paul, MN or her successor.

**D. Consumer Assistance Partner Payments.** DHS will:

1. At MNSure's request, provide timely input on all consumer assistance partner compensation model decisions.
2. Provide approval for any modifications to Consumer Assistance Partner compensation rates proposed by MNSure.
3. Using payment reports provided by MNSure, review and approve within two weeks, as appropriate, all consumer assistance partner payments as recommended by MNSure.
4. Submit all approved consumer assistance partner payments to DHS Financial Operations Division.
5. DHS Financial Operations Division to make payments with 72 hours of submission of the approved payment report.
6. Work with MNSure to ensure Consumer Assistance Partner compensation payments are appropriate.
7. Consistent with Section 1.5 (Internal Audits) of this Agreement, cooperate with MNSure in audits of Consumer Assistance Partner payments. In the event of an audit initiated by DHS that requires cooperation and assistance from MNSure, DHS shall provide reasonable notice of any such audit, and work with MNSure to avoid the disruption of business operations during the audit.
8. DHS Contact: Marty Cammack, Director, Financial Operations, 540 Cedar Avenue, St, Paul, MN, or his successor.

**3. Mutual Responsibilities.** DHS and MNSure will coordinate operations of the consumer assistance programs according to above sections. Coordination responsibilities include:

**A. Resources.**

1. DHS Health Care Administration will designate a liaison to the consumer assistance programs.
2. MNSure will designate a supervisor to ARC staff.

**B. Communication.** DHS and MNSure will have regular check-in meetings on the status of the navigator program, including discussion of program metrics.

# Amendment No.2 to Interagency Agreement 201592

Contract Start Date:	October 14, 2021	Original Contract:	\$13,073,259
Original Contract Expiration Date:	6/30/2023	Previous Amendment(s) Total:	\$0
Current Contract Expiration Date:	6/30/2023	This Amendment:	\$113,000
Requested Contract Expiration Date:	N/A	Total Contract Amount:	\$13,186,259

**This amendment** ("Amendment") is by and between Minnesota Department of Human Services, Commissioner's Office Division, (hereinafter DHS) and the Chief Executive Officer of the Minnesota Health Insurance Marketplace (hereinafter "MNSure").

## Recitals

1. DHS and MNSure have an agreement identified as IAK-201592 ("Agreement") to allow DHS to provide standard, centralized administrative services to MNSure;
2. DHS and MNSure agree that the Agreement should be modified to update the budget for the actual costs of FY 2022 for METS Services and to update DHS' authorized representatives; and
3. DHS and MNSure are willing to amend the Agreement as stated below.

## Contract Amendment #2

In this Amendment, changes to pre-existing Contract language will use ~~strike through~~ for deletions and underlining for insertions.

**REVISION 1. Clause 1.1. B. "Authorized Representatives."** is amended as follows:

### B. Authorized Representatives.

1. DHS' authorized representative in regards to human resource services is ~~Connie Jones-Kamaria~~ Kassim-Grigsby, Human Resources Director, or her successor.
2. MNSure's authorized representative in regards to human resource services is Dave Rowley, General Counsel, or his successor.
3. Each representative shall have final authority for acceptance of human resource services of the other party and shall have responsibility to ensure that all payments due to the other party with respect to human resource services are made pursuant to the terms of this Agreement.

**REVISION 2. Clause 1.2. B. "Authorized Representatives."** is amended as follows:

### B. Authorized Representatives.

1. DHS's authorized representative in regards to financial operations is ~~Joe Jarosz, Accounting Operations Manager,~~ Carmen Patton-Minder, Financial Operations Director, or ~~his~~ their

successor.

2. MNSure's authorized representative in regards to financial operations is Gerald Wood, Accounting Operations Director, or his successor.
3. Each representative shall have final authority for acceptance of payroll and accounts payable services of the other party and shall have responsibility to ensure that all payments due to the other party with respect to payroll and accounts payable services are made pursuant to the terms of this Agreement.

**REVISION 3. Clause 1.7. B. "Authorized Representatives."** is amended as follows:

**B. Authorized Representatives.**

1. DHS' authorized representative in regards to issuance operation services is ~~Joe Jarosz, FOD- Accounting Operations Director,~~ Mike LaValle, Procurement Supervisor, or his successor.
2. MNSure's authorized representative in regards to issuance operation services is Gerald Wood, Accounting Operations Director, or his successor.
3. Each representative shall have final authority for acceptance of issuance operation services of the other party and shall have responsibility to ensure that all payments due to the other party with respect issuance operation services are made pursuant to the terms of this Agreement

**REVISION 4. Clause 2.1 B. "Authorized Representatives."** is amended as follows:

**B. Authorized Representatives.**

1. DHS' authorized representative in regards to METS System Operations services is ~~Anna-Minge~~ David Greeman, Chief Financial Officer, or ~~her~~ their successor.
2. MNSure's authorized representative in regards METS System Operations services is Kari Koob, Chief Financial Officer, or her successor.
3. Each representative shall have final authority for acceptance of METS System Operations services of the other party and shall have responsibility to ensure that all payments due to the other party with respect to METS System Operations services are made pursuant to the terms of this Agreement

**REVISION 5. Clause 2.2 B. "Authorized Representatives."** is amended as follows:

**B. Authorized Representatives.**

1. DHS' authorized representative in regards to METS System Development-QHP services is ~~Anna-Minge~~ David Greeman, Chief Financial Officer, or ~~her~~ their successor.
2. MNSure's authorized representative in regards to METS System Development- QHP services is Kari Koob, Chief Financial Officer, or her successor.
3. Each representative shall have final authority for acceptance of METS System Development-QHP services of the other party and shall have responsibility to ensure that all payments due to the other party with respect to METS System Development-QHP services are made

pursuant to the terms of this Agreement.

**REVISION 6. Clause 3.2. "Authorized Representatives."** is amended as follows:

**3.2 Authorized Representatives.**

1. DHS' authorized representative in regards to occupancy and IT support indirect costs is ~~Marty Cammack~~ Carmen Patton-Minder, Financial Operations Director, or ~~her~~ their successor.
2. MNSure's authorized representative in regards to occupancy and IT support indirect costs is Kari Koob, Chief Financial Officer, or her successor.
3. Each representative shall have final authority for acceptance of IT support services of the other party and shall have responsibility to ensure that all payments due to the other party with respect to IT support services are made pursuant to the terms of this Agreement

**REVISION 7. Clause 4.A.3. "Scope."** is amended as follows:

3. DHS' and MNSure's roles and responsibilities in the operation, support, and implementation of the Consumer Assistance Programs, including the Navigator Program and Certified Application Counselor Program, and the Assistor Resource Center shall be governed by Revised Exhibit E, Consumer Assistance Program, which is attached and incorporated into this Agreement.

**REVISION 8. Clause 5.B. "Consideration"** is amended as follows:

- B. Consideration.** Consideration for all services performed by DHS pursuant to this Agreement shall be paid by MNSure in accordance with the allocations set forth in Revised Exhibit A, Budget; as amended, which is attached and incorporated into this Agreement.

**REVISION 9. Clause 5.D. "Total Obligation"** is amended as follows:

**D. Total Obligation.**

1. **MNSure Business Operations Services.** The total obligation of MNSure for all compensation and reimbursements to DHS for non-IT related services under this Agreement shall not exceed **two million two hundred and five thousand dollars (\$2,205,000)**, unless otherwise stated in Revised Exhibit A, Budget as amended.
2. **METS Services.** The total obligation of MNSure for all compensation and reimbursements to DHS for IT related services under this Agreement shall not exceed ~~ten million five hundred and eighteen thousand and two hundred fifty nine dollars (\$10,518,259)~~, ten million six hundred and thirty-one thousand, two hundred fifty-nine dollars (\$10,631,259), unless otherwise stated in Revised Exhibit A, Budget; as amended.
3. **Occupancy and IT Support Indirect Costs.** The total obligation of MNSure for all compensation and reimbursements to DHS for occupancy and IT support indirect costs under this Agreement shall not exceed **three hundred and fifty thousand dollars (\$350,000.00)**, unless otherwise stated in Revised Exhibit A, Budget as amended.

**REVISION 10. Clause 5.E. "Advance Payments"** is amended as follows:

- E. Advance Payments.** MNsures and DHS's Chief Financial Officers, or their successors, may, based on estimated, invoices, authorize advance payments between MNsures and DHS for the limited purpose of addressing cash flow issues resulting from quarterly PACAP and COCAS procedures. Advance payments made under this Section must be settled against the next invoice and shall not exceed line item amounts set forth in Revised Exhibit A, Budget as amended.

**EXCEPT AS AMENDED HEREIN, THE TERMS AND CONDITIONS OF THE ORIGINAL AGREEMENT AND ALL PREVIOUS AMENDMENTS REMAIN IN FULL FORCE AND EFFECT AND ARE INCORPORATED INTO THIS AMENDMENT BY REFERENCE.**


***REMAINDER OF PAGE INTENTIONALLY LEFT BLANK***  
***SIGNATURE PAGE FOLLOWS***



**APPROVED:**

**1. STATE ENCUMBRANCE VERIFICATION**

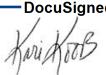
*Individual certifies that funds have been encumbered as required by Minnesota Statutes, chapter 16A and section 16C.05.*

By:  \_\_\_\_\_  
DocuSigned by: 53AD6200B0B8428...

Date: 9/21/2022 \_\_\_\_\_

SWIFT Contract No: 201592 \_\_\_\_\_

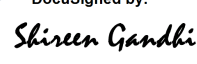
**2. MNsure**

By with delegated authority):  \_\_\_\_\_  
DocuSigned by: F3466CF591CC40D...

Title: CFO \_\_\_\_\_

Date: 9/30/2022 \_\_\_\_\_

**3. MN Department of Human Services**

By (with delegated authority):  \_\_\_\_\_  
DocuSigned by: 47351621927240A...

Title: Deputy Commissioner, Agency Effectiveness \_\_\_\_\_

Date: 10/5/2022 \_\_\_\_\_

**Revised EXHIBIT A – Interagency Agreement Budget**

Section (i.e. services to be provided)	Basis for Amount Charged	Authorized Representative		Totals	
		MNsure / Kari Koob	DHS / <del>Anna Minge David Greeman</del> or successor	2 <sup>nd</sup> -4 <sup>th</sup> quarters FY2022	FY2023
1.1 Human Resources	Fixed	Dave Rowley	<del>Connie Jones-Kamaria Kassim-Grigsby</del>	150,000	200,000
1.2 Financial Operations	Fixed	Gerald Wood	<del>Joe Jarosz-Carmen Patton-Minder</del>	112,500	150,000
1.3 Procurement	Fixed	Katie DeGrio Channing	Mike LaValle	63,750	85,000
1.4 Contracts	Fixed	Katie DeGrio Channing	Song Lyfoung	11,250	15,000
1.5 Background Studies	Variable	Christina Wessel	Dawn Davis	18,750	25,000
1.6 Fair Hearing and Appeals	Variable	Katie DeGrio Channing	Steven Collins	375,000	500,000
1.7 Issuance Operations Center	Variable	Gerald Wood	<del>Joe Jarosz</del> Mike LaValle	213,750	285,000
<b>Total Business Operation Services</b>				<b>945,000</b>	<b>1,260,000</b>
2.1 METS System Operations	Variable	Kari Koob	<del>Anna Minge David Greeman-or successor</del>	4,620,087	5,898,172
2.2 METS System Development-QHP	Variable	Kari Koob	<del>Anna Minge David Greeman-or successor</del>	<del>0 \$113,000</del>	0
<b>Total METS Services</b>				<b><del>4,620,087</del> 4,733,087</b>	<b>5,898,172</b>
<b>3. Occupancy and IT Support Indirect Costs</b>	Fixed	Kari Koob	<del>Marty Cammack</del> Carmen Patton-Minder	<b>150,000</b>	<b>200,000</b>
<b>Total Interagency Agreement</b>				<b><del>5,715,087</del> 5,828,087</b>	<b>7,358,172</b>
					13,073,259
					13,186,259

**Revised Exhibit E - Consumer Assistance Program**

1. **MNsure's Responsibilities.** MNsure will operate the Consumer Assistance Programs, including the Navigator Program, Certified Application Counselor program, and the Assister Resource Center ("ARC"). Operational responsibilities include:
  - A. **Contracting.** MNsure will:
    1. Process all consumer assistance partner applications and contracts;
    2. Specifically identify DHS as a third-party beneficiary in all Consumer Assistance Partner contracts including, Certified Application Counselor Services Agreements, and Joint Powers and Grant Navigator/In-Person Assister Agreements.
    3. Request input from DHS's Contracts division on the creation and modification of all consumer assistance partner contract templates.
  - B. **Training, resource pages and manual.** MNsure will:
    1. Develop, implement, and maintain certification and recertification training for all consumer assistance partners
    2. Request input and content from DHS' Health Care Administration on all consumer assistance partner training related to public programs.
    3. Update and maintain the navigator resource webpages.
  - C. **Certification.** MNsure will:
    1. Process all consumer assistance partner certification, recertification, and decertification.
    2. Resolve all complaints against consumer assistance partners.
  - D. **Customer Service and Support.** MNsure will:
    1. Provide customer services and support to consumer assistance partners through the ARC.
    2. Oversee supervision, hiring, work direction and priority setting as it relates to staffing and work activities of the ARC.
    3. Develop, implement, and maintain operational support for all consumer assistance partners.
    4. Obtain input and approval from DHS Health Care Administration on all consumer assistance partner communications related to public programs.
  - E. **Compensation.** MNsure will:
    1. Seek approval from DHS FOD for all consumer assistance partner payments and provide necessary data.

2. Request input from DHS on all consumer assistance partner compensation model decisions.
3. Maintain all consumer assistance partners' compensation according set forth in the Consumer Assistance Partner contracts, and not make any modifications to Consumer Assistance Partner compensation rates without the explicit approval of DHS.
4. Implement controls to ensure Consumer Assistance Partner compensation payments are appropriate and audit as needed to safeguard against potential fraud or misuse.
5. Consistent with Clause 1.5 (Internal Audits) of this Agreement, cooperate with DHS audits of consumer assistance partner payments. In the event of an audit of Consumer Assistance Partner payments initiated by MNSure that requires cooperation and assistance from DHS, MNSure shall provide reasonable notice of such an audit. MNSure will work with DHS to avoid disruption of DHS business operations during audit.
6. Be responsible for working with MN.IT staff to develop payment reports, clean data, run report, and develop and send payment statements.
7. Respond to all questions about and facilitate resolving issues regarding compensation.

**2. DHS' Responsibilities.** DHS will support the operations of consumer assistance programs, including the Navigator program and Certified Application Counselor program. Support responsibilities include:

**A. Contracting.** DHS will:

1. Participate as third-party beneficiary to all consumer assistance partner contracts with MNSure, including Certified Application Counselor Services Agreements, and Joint Powers and Grant Navigator/In-Person Assister Agreements.
2. Provide input from DHS Contracts division on all consumer assistance partner contract templates.
3. Provide review on all requested changes to templates.
4. DHS Contact: Song Lyfoung, Director, Contracts, Procurement, and Legal Compliance, 444 Lafayette Road, St. Paul, MN, or her successor.

**B. Training, Resource Pages and Manual.** DHS will:

1. Provide reviewers for training content developed by MNSure. This review will occur on a mutually agreed-upon schedule.
2. Review public program related processes within the navigator manual and navigator resource webpages on a mutually-agreed upon schedule.

3. DHS Contact: Christina Cox; Supervisor, Training and Partner Relations, HCEO, 540 Cedar Avenue, St. Paul, MN, or her successor.

**C. Customer Service and Support.** DHS will:

1. Respond to public program policy questions from the ARC within ten working days through the DHS' HCEO County Relations Resource Center.
2. Provide timely input and approval from DHS HCEO on all consumer assistance partner communications related to public programs,
3. Provide Assister Resource Center (ARC) staff and the ARC supervisor with access to SIR, MMIS; MAXIS and DHS FileNet upon request to provide consumer assistance partner support for public programs per appropriate law and policy.
4. Designate a point person and backup for ARC questions that are more time sensitive for the County Relations Resource Center. These staff will be available during regular DHS business hours (8am-4:30pm),
5. DHS Contact: Isaac Akpojotor, Supervisor, Resource Center Systems Support, HCEO, 540 Cedar Avenue, St. Paul, MN or her successor.

**D. Consumer Assistance Partner Payments.** DHS will:

1. At MNSure's request, provide timely input on all consumer assistance partner compensation model decisions.
2. Provide approval for any modifications to Consumer Assistance Partner compensation rates proposed by MNSure.
3. Using payment reports provided by MNSure, review and approve within two weeks, as appropriate, all consumer assistance partner payments as recommended by MNSure.
4. Submit all approved consumer assistance partner payments to DHS Financial Operations Division.
5. DHS Financial Operations Division to make payments with 72 hours of submission of the approved payment report.
6. Work with MNSure to ensure Consumer Assistance Partner compensation payments are appropriate.
7. Consistent with Section 1.5 (Internal Audits) of this Agreement, cooperate with MNSure in audits of Consumer Assistance Partner payments. In the event of an audit initiated by DHS that requires cooperation and assistance from MNSure, DHS shall provide reasonable notice of any such audit, and work with MNSure to avoid the disruption of business operations during the audit.
8. DHS Contact: ~~Marty Cammack, Director, Financial Operations~~ Carmen Patton-Minder, Financial Operations Division Director, 540 Cedar Avenue, St, Paul, MN, or ~~his~~ their successor.

**3. Mutual Responsibilities.** DHS and MNsure will coordinate operations of the consumer assistance programs according to above sections. Coordination responsibilities include:

**A. Resources.**

1. DHS Health Care Administration will designate a liaison to the consumer assistance programs.
2. MNsure will designate a supervisor to ARC staff.

B. Communication. DHS and MNsure will have regular check-in meetings on the status of the navigator program, including discussion of program metrics.

## **DHS OF MINNESOTA DEPARTMENT OF HUMAN SERVICES INTERAGENCY AGREEMENT WORKSHEET (Not Part of the Agreement)**

### **Originator of agreement, complete this section:**

Total amount of interagency agreement: \$\_\_\_\_\_

Proposed Start Date: 10 / \_1\_ / \_21\_

Proposed End Date: \_06\_ /30\_ / \_23\_

SFY\_\_ - SWIFT FinDeptID: H55EB \_\_\_\_\_ \$\_\_\_\_\_ amount

If multiple FinDeptID's will be used to fund this, fill that in below and then define the split between funds.

SFY\_\_ - SWIFT FinDeptID: H55EB \_\_\_\_\_ \$\_\_\_\_\_ amount

SFY\_\_ - SWIFT FinDeptID: H55EB \_\_\_\_\_ \$\_\_\_\_\_ amount

Reference the contract number and purchase order number assigned below when processing invoices for this agreement. Send invoices to FOD – 0940

### **Contract Coordinator, complete this section:**

SWIFT Vendor # for Other State Agency: H60000000

SWIFT Contract #: IAK % 201563

SWIFT Purchase Order #: N/A

Buyer Initials: \_\_\_\_\_ Date Encumbered: \_\_\_\_\_

Individual signing certifies that funds have been encumbered as required by MS § 16A15.

## INTERAGENCY AGREEMENT between DHS and MNSure for MNSure Participation in the Administration of the Minnesota State Plan for Services Under Title XIX

---

### **Recitals:**

**WHEREAS**, the Department of Human Services, hereinafter DHS, is empowered to enter into interagency agreements pursuant to Minnesota Statutes § 471.59, Subdivision 10; and

**WHEREAS**, MNSure is empowered to enter into interagency agreements pursuant to Minnesota Statutes § 471.59, Subdivision 10; and

WHEREAS, DHS is designated as the Medicaid Agency for the State of Minnesota and, as such, is responsible for management and oversight of Medical Assistance (MA), which is Minnesota's Medicaid program; and

WHEREAS, The day-to-day operations of MNSure play an important role in the Department of Human Services' outreach and enrollment strategies for Minnesotans seeking the services of public health coverage programs and services, including MinnesotaCare and Medicaid; and

WHEREAS, DHS and MNSure are formally recognizing that work performed by MNSure benefits public health programs and MNSure expenditures will be included, as necessary, in DHS' public assistance, cost allocation plan, and operational advance planning documents.

**NOW, THEREFORE, it is agreed:**

### **1. Duties:**

#### **1.1 MNSure's Duties:**

MNSure shall: help DHS to outreach, identify, intake, accept, determine eligibility for, and formally enroll eligible individuals and their families into the entire range of public and private health insurance programs in Minnesota, including individual qualified health insurance plans, the basic health insurance plan (MinnesotaCare), and medical assistance services available for those qualifying for Medicaid.

MNSure shall provide a variety of services related to Medicaid eligibility determination and enrollment activities including, but not limited to application, on-going case maintenance and renewal activities, policy, outreach and post-eligibility activities, and other activities necessary for administration of the state plan for services under Title XIX.

#### **1.2. DHS's DUTIES:**

DHS shall: obtain annual appropriations for the ongoing operation of MNSure, and shall claim the federal share of any eligible expenditures via operation of its amended public assistance cost allocation plan and operational advance planning document.



## **2. CONSIDERATION AND TERMS OF PAYMENT**

**2.1 Consideration.** Consideration for all services performed by MNSure pursuant to this agreement shall be paid by DHS as follows: There is no encumbrance under this agreement. The basis for billing will be the operational advance planning document and the quarterly operation of the public assistance cost allocation plan. It is further understood that any billing will be based on the actual cost incurred.

**2.2 Terms of Payment.** Payment shall be made to MNSure from DHS within 30 days after DHS has completed its quarterly COCAS procedure.

**3. Conditions of Payment.** All services provided by MNSure pursuant to this agreement shall be performed to the satisfaction of DHS, as determined at the sole discretion of its authorized representative.

**4. Terms of Agreement.** This agreement shall be effective on October 1, 2021 **or upon the date that the final required signature is obtained, pursuant to Minnesota Statutes, section 16C.05, subdivision 2, whichever occurs later**, and shall remain in effect through June 30, 2023, or until all obligations set forth in this agreement have been satisfactorily fulfilled, whichever occurs first.

**5. Cancellation.** This agreement may be canceled by the DHS or MNSure at any time, with or without cause, upon thirty (30) days written notice to the other party. In the event of such a cancellation, the MNSure shall be entitled to payment, determined on a pro rata basis, for work or services satisfactorily performed.

**6. Authorized Representatives.** DHS's authorized representative for the purposes of administration of this agreement is Dave Greeman or successor. MNSure's authorized representative for the purposes of administration of this agreement is Kari Koob, CFO, or successor. Each representative shall have final authority for acceptance of services of the other party and shall have responsibility to insure that all payments due to the other party are made pursuant to the terms of this agreement.

**7. Assignment.** Neither MNSure nor DHS shall assign or transfer any rights or obligations under this agreement without the prior written consent of the other party.

**8. Amendments.** Any amendments to this agreement shall be in writing, and shall be executed by the same parties who executed the original agreement, or their successors in office.

**9. Liability.** MNSure and DHS agree that each party will be responsible for its own acts and the results thereof to the extent authorized by law and shall not be responsible for the acts of the other and the results thereof. MNSure and DHS liability shall be governed by the provisions of the Minnesota Tort Claims Act, Minnesota Statutes, section 3.736, and other applicable law.

## **10. INFORMATION PRIVACY AND SECURITY.**

Information Privacy and Security shall be governed by the existing Data Sharing and Business Associate Agreement between MNsure and DHS, identified as DSK %187696, and any succeeding Data Sharing Agreement, which is incorporated into this agreement by reference.

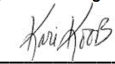
## **11. Other Provisions.**

None.

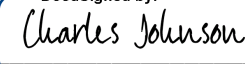
IN WITNESS WHEREOF, the parties have caused this contract to be duly executed intending to be bound thereby

APPROVED:

**1. MNsure**

DocuSigned by:  
By:   
F3466CF591CC40D...  
Title: CFO  
Date: 9/29/2021

**2. DHS**

DocuSigned by:  
By:   
E336517A7B0D415...  
*With delegated authority*  
Title: Deputy Commissioner  
Date: 9/29/2021

Distribution:

DHS – Original (fully executed) contract

MNsure

Contracting & Legal Compliance, Contracts Unit- #0238



## **DATA SHARING AND BUSINESS ASSOCIATE AGREEMENT TERMS AND CONDITIONS**

---

This Data Sharing and Business Associate Agreement, and amendments and supplements thereto (“Agreement”), is between the State of Minnesota Department of Human Services (“DHS”) and Minnesota Insurance Marketplace a/k/a MNsure (“MNsure”), collectively referred to as “parties”.

### **RECITALS**

This Agreement sets forth the terms and conditions in which parties will share data with and permit the other party to Use or Disclose Protected Information that the parties are legally required to safeguard pursuant to the Minnesota Government Data Practices Act (“MGDPA”) under Minnesota Statutes, Chapter 13, the Health Insurance Portability and Accountability Act rules and regulations codified at 45 C.F.R. Parts 160, 162, and 164 (“HIPAA”), and other Applicable Safeguards.

The parties agree to comply with all applicable provisions of the MGDPA, HIPAA, and any other Applicable Safeguard that applies to the Protected Information.

DHS is the primary state agency to help people meet their basic needs by providing or administering a variety of services for children, people with disabilities, and older Minnesotans.

DHS is the designated Medicaid Agency for the state of Minnesota and is responsible for the management and oversight of Medical Assistance (MA), MinnesotaCare, and other Minnesota Health Care Programs.

DHS is a “health care provider” and a “covered entity” under the Health Insurance Portability and Accountability Act (HIPAA) pursuant to 45 C.F.R. § 160.103.

MNsure is the state of Minnesota’s state health benefit exchanged as described in section 1311 of the Patient Protection and Affordable Care Act, Public Law 111-148.

MNsure and DHS share decision-making in conjunction with MNIT Services for the Minnesota Eligibility Technology System (METS).

To carry out their duties under the Interagency Agreements between the parties to implement and administer the Minnesota Insurance Marketplace and Minnesota Health Care Programs (“Interagency Agreements”), MNsure and DHS are required to share Protected Information and Protected Health Information with each other, as defined in this Agreement.

MNsure is permitted to share the protected information with DHS pursuant to Minnesota Statutes, section 62V.06, subdivisions 5(a)(4) and 5(b)(4) and 45 C.F.R. § 155.260.

MNsure agrees it is a “business associate” of DHS, as defined by HIPAA under 45 C.F.R. § 160.103, “Definitions,” for the limited purpose of carrying out health care eligibility operations and administration on behalf of DHS. The Protected Health Information disclosed to MNsure is subject to the Health Insurance Portability Accountability Act (HIPAA) is permitted by 45 C.F.R. § 164.502(e)(1)(i), “Standard: Disclosures to Business Associates.”

MNsure and DHS are directly liable and may be subject to civil penalties for failing to safeguard electronic Protected Health Information in accordance with the HIPAA Security Rule, Subpart C of 45 C.F.R. Part 164, “Security and Privacy.”

DHS is permitted to share protected health information with MNsure by 45 C.F.R. §§ 164.502(a)(1)(ii) and 164.506(c)(1) for DHS’ health care operations.

Minnesota Statutes, section 13.46, subdivision 1(c), allows DHS to enter into agreements to make the other entity part of the “Welfare System.” It is the intention that MNsure be made part of the welfare system for the limited purpose described in the Interagency Agreements and this Agreement.

Pursuant to Minnesota Statutes, section 13.46, subdivision 2(a)(5), DHS is permitted to release private data on individuals to personnel of the welfare system who require the data to verify an individual’s identity, the amount of assistance, and the need to provide services to an individual or family across programs; and evaluate the effectiveness of programs.

Pursuant to Minnesota Statutes, section 13.46, subdivision 2(a)(6), DHS is permitted to release private data on individuals to administer federal funds and programs.

Therefore, the parties agree as follows:

#### **DEFINITIONS**

- A. “Agent” means the parties’ employees, contractors, subcontractors, and other non-employees and representatives.
- B. “Applicable Safeguards” means the state and federal safeguards listed in subsection 6.1.A of this Agreement.
- C. “Breach” means the acquisition, access, use, or disclosure of unsecured Protected Health Information in a manner not permitted by HIPAA, which compromises the security or privacy of Protected Health Information.
- D. “Business Associate” shall generally have the same meaning as the term “business associate” found in 45 C.F.R. § 160.103, and in reference to the party in the Agreement, shall mean MNsure.
- E. “Disclose” or “Disclosure” means the release, transfer, provision of access to, or divulging in any manner of information by the entity in possession of the Protected Information.

- F. "HIPAA" means the rules and regulations codified at 45 C.F.R. Parts 160, 162, and 164.
- G. "Individual" means the person who is the subject of protected information.
- H. "Privacy Incident" means a violation of an information privacy provision of any applicable state and federal law, statute, regulation, rule, or standard, including those listed in the Agreement.
- I. "Protected Information" means any information, regardless of form or format, which is or will be Used by DHS or MNsure under the Agreement that is protected by federal or state privacy laws, statutes, regulations, policies, or standards, including those listed in this Agreement. This includes, but is not limited to, individually identifiable information about a State, county or tribal human services agency client or a client's family member. Protected Information also includes, but is not limited to, Protected Health Information, as defined below, and Protected Information maintained within or accessed via a State information management system, including a State "legacy system" and other State application.
- J. "Protected Health Information" is a subset of Protected Information (defined above) and has the same meaning as the term "protected health information" found in 45 C.F.R. § 160.103. For the purposes of this Agreement, it refers only to that information that is received, created, maintained, or transmitted between DHS and MNsure as a Business Associate for the limited purpose of carrying out health care eligibility operations and administration on behalf of DHS.
- K. "Responsible Party" is the agency whose employee, volunteer, agent, vendor, contractor or subcontractor actions causes the Breach, Privacy Incident, and/or Security Incident. For purposes of this Agreement, if the parties to this Agreement disagree or cannot determine the cause of an incident, or if a third party caused a security incident, both parties to this Agreement will be deemed the Responsible Party for the Breach, Privacy Incident, and/or Security Incident, and the parties will work cooperatively to agree on one party to take the lead with coordination and assistance from the other party.
- L. "Security Incident" means the attempted or successful unauthorized accessing, Use, or interference with system operations in an information management system or application. "Security Incident" does not include pings and other broadcast attacks on a system's firewall, port scans, unsuccessful log-on attempts, denials of service, and any combination of the above, provided that such activities do not result in the unauthorized exposure, viewing, obtaining, accessing, or Use of Protected Information.
- M. "Use" or "Used" means any activity involving Protected Information including its creation, collection, access, acquisition, modification, employment, application, utilization, examination, analysis, manipulation, maintenance, dissemination, sharing, Disclosure, transmission, or destruction. "Use" includes any of these activities whether conducted manually or by electronic or computerized means.
- N. "User" means an agent of either party, who has been authorized to use Protected Information.

**1. TERM OF AGREEMENT.**

**1.1 Effective date.** The effective date of this Agreement is **January 1, 2021**.

**1.2 Expiration date.** The expiration date of this Agreement is **December 31, 2023**, or until all obligations set forth in this Agreement have been satisfactorily fulfilled, whichever occurs first.

**2. INFORMATION EXCHANGED.**

**2.1** This Agreement shall govern the data that will be exchanged between MNSure and DHS, which may include:

- A. patient data relating to DHS' Minnesota Health Care Programs (MHCP);
- B. the provision of health care to MHCP beneficiaries and MNSure clients;
- C. past, present, or future payment for the provision of health care to MHCP beneficiaries and MNSure clients;
- D. data on individuals participating in MNSure as defined in Minnesota Statutes, section 62V.06;
- E. data on employers participating in MNSure; and
- F. "not public data" as defined in Minnesota Statutes, section 13.02.

**3. TIME.**

The parties will perform their duties within the time limits established in this Agreement unless prior written approval is obtained from the other party.

**4. CONSIDERATION AND PAYMENT.**

There will be no funds obligated by either party under this Agreement. Each party will be responsible for its own costs in performing its stated duties.

**5. AUTHORIZED REPRESENTATIVES.**

**5.1 DHS.** DHS's authorized representative is **Donna Watz, Deputy General Counsel Chief Privacy Official**, donna.m.watz@state.mn.us, or her successor. MNSure shall make any notice or contact to DHS required by this Agreement to DHS's authorized representative.

**5.2 MNSure.** MNSure's Authorized Representative is **Emily Cleveland, Legal Director and Privacy Officer**, emily.j.cleveland@state.mn.us, or her successor. DHS shall make any notice or contact to MNSure required by this Agreement to MNSure's authorized representative.

**6. INFORMATION PRIVACY AND SECURITY**

MNSure and DHS must comply with the MGDPA, HIPAA, and all other Applicable Safeguards as they apply to all data provided by MNSure or DHS under this Agreement, and as they apply to all data created, collected, received, stored, used, maintained, or disseminated by MNSure or DHS under this Agreement. The civil remedies of Minn. Stat. § 13.08, "Civil Remedies," apply to MNSure and DHS. Additionally, the remedies of HIPAA apply to the release of data governed by HIPAA.

**6.1 Compliance with Applicable Safeguards.**

- A. State and Federal Safeguards.** The parties acknowledge that the Protected Information to be shared under the terms of the Agreement may be subject to one or more of the laws, statutes, regulations, rules, policies, and standards, as applicable and as amended

or revised (“Applicable Safeguards”), listed below, and agree to abide by the same.

1. Health Insurance Portability and Accountability Act rules and regulations codified at 45 C.F.R. Parts 160, 162, and 164 (“HIPAA”);
2. Medicaid Information Safeguards (42 C.F.R. § 431 Subpart F);
3. Minnesota Government Data Practices Act (Minn. Stat. Chapter 13);
4. Minnesota Health Records Act (Minn. Stat. § 144.291–144.34);
5. Data Practices section of the MNsure Act (Minn. Stat § 62V.06)
6. Confidentiality of Alcohol and Drug Abuse Patient Records (42 U.S.C. § 290dd-2, “Confidentiality of Records,” and 42 C.F.R. Part 2, “Confidentiality of Substance Use Disorder Patient Records”);
7. Tax Information Security Guidelines for Federal, State and Local Agencies (26 U.S.C. § 6103, “Confidentiality and Disclosure of Returns and Return Information,” and Internal Revenue Service Publication 1075;
8. U.S. Privacy Act of 1974;
9. Computer Matching Requirements (5 U.S.C. § 552a, “Records Maintained on Individuals”);
10. Social Security Data Disclosure (section 1106 of the Social Security Act: 42 USC § 1306, “Disclosure of information in Possession of Social Security Administration or Department of Health and Human Services”);
11. Disclosure of Information to Federal, State and Local Agencies (DIFSLA Handbook, Internal Revenue Service Publication 3373);
12. Final Exchange Privacy Rule of the Affordable Care Act (45 C.F.R. § 155.260, “Privacy and Security of Personally Identifiable Information,”);
13. NIST Special Publication 800-53, “Security and Privacy Controls for Federal Information Systems and Organizations,” Revision 4 (NIST.SP.800-53r4); and,
14. All state of Minnesota [“Enterprise Information Security Policies and Standards.”](#)<sup>1</sup>

The parties further agree to comply with all other laws, statutes, regulations, rules, and standards, as amended or revised, applicable to the exchange, Use and Disclosure of data under the Agreement.

- B. Statutory Amendments and Other Changes to Applicable Safeguards.** The Parties agree to take such action as is necessary to amend the Agreement from time to time as is necessary to ensure, current, ongoing compliance with the requirements of the laws listed in this Section or in any other applicable law.

## 6.2 The Parties’ Data Responsibilities

- A. Use of Protected Information.** Each party shall:

1. disclose Protected Information only as authorized by law to the other party for its use or disclosure;
2. obtain any consent or authorization that may be necessary for it to disclose Protected Information with the other party; and
3. refrain from asking the other party to use or disclose Protected Information in a manner that would violate applicable standards or would be impermissible if the use or disclosure were performed by the party.

<sup>1</sup> See <https://mn.gov/mnit/government/policies/security/>



**B. Use Limitation.**

1. **Restrictions on Use and Disclosure of Protected Information.** Except as otherwise authorized in the Agreement, the parties may only use or disclose Protected Information as minimally necessary to provide the services to the other party as described in the Agreement, or as otherwise required by law, provided that such use or disclosure of Protected Information, if performed by the party, would not violate the Agreement, HIPAA, or state and federal statutes or regulations that apply to the Protected Information.
2. **Federal tax information.** To the extent that Protected Information used under the Agreement constitutes "federal tax information" (FTI), both parties shall ensure that this data only be used as authorized under the Patient Protection and Affordable Care Act, the Internal Revenue Code, 26 U.S.C. § 6103, and IRS Publication 1075.

**C. Individual Privacy Rights.** The parties shall ensure Individuals are able to exercise their privacy rights regarding Protected Information, including but not limited to the following:

1. **Complaints.** The parties shall work cooperatively and proactively with each other to resolve complaints received from an Individual; from an authorized representative; or from a state, federal, or other health oversight agency.
2. **Amendments to Protected Information Requested by Data Subject Generally.** Within ten (10) business days, one party must forward to the other party any request to make any amendment(s) to Protected Information in order for the parties to satisfy their obligations under Minnesota Statutes, section 13.04, "Rights of Subjects of Data," subd. 4. If the request to amend Protected Information pertains to Protected Health Information, then the parties must also make any amendment(s) to Protected Health Information as directed or agreed to by the parties pursuant to 45 C.F.R. § 164.526, "Amendment of Protected Health Information," or otherwise act as necessary to satisfy DHS or MNsure's obligations under 45 C.F.R. § 164.526 (including, as applicable, Protected Health Information in a designated record set).

**D. Background Review and Reasonable Assurances of Agents.**

1. **Reasonable Assurances.** Each party represents that, before any Agent is allowed to Use or Disclose Protected Information, each party has conducted and documented a background review of the Agent sufficient to provide the other party with reasonable assurances that the Agent will fully comply with the terms of the Agreement and Applicable Safeguards.
2. **Documentation.** Each party shall make available documentation required by this Section upon request.

**E. Ongoing Responsibilities to Safeguard Protected Information.**

1. **Privacy and Security Safeguards.** Each party shall develop, maintain, and enforce policies, procedures, and administrative, technical, and physical safeguards that

comply with the Applicable Safeguards to ensure the privacy and security of the Protected Information, and to prevent the Use or Disclosure of Protected Information, except as expressly permitted by the Agreement.

2. **Electronic Protected Information.** Each party shall implement and maintain appropriate safeguards with respect to electronic Protected Information, and comply with Subpart C of 45 C.F.R. Part 164 (HIPAA Security Rule) with respect to prevent the Use or Disclosure other than as provided for by the Agreement.
  3. **Monitoring Agents.** Each party shall ensure that any Agent to whom the party Discloses Protected Information on behalf of the other party, or whom the party employs or retains to create, receive, Use, store, Disclose, or transmit Protected Information on behalf of the other party, agrees in writing to the same restrictions and conditions that apply to the party under the Agreement with respect to such Protected Information; and, for protected health information, in accordance with 45 C.F.R. §§ 164.502, "Use and Disclosure of Protected Health Information: General Rules," subpart (e)(1)(ii) and 164.308, "Administrative Safeguards," subpart (b)(2).
  4. **Encryption.** According to the state of Minnesota's "[Enterprise Information Security Policies and Standards](#),"<sup>2</sup> both parties must use encryption to store, transport, or transmit Protected Information and must not use unencrypted email to transmit Protected Information.
  5. **Minimum Necessary Access to Protected Information.** Each party shall ensure that its Agents acquire, access, Use, and Disclose only the minimum necessary Protected Information needed to complete an authorized and legally permitted activity.
  6. **Training and Oversight.** Each party shall ensure that Agents are properly trained and comply with all Applicable Safeguards and the terms of the Agreement.
- F. **Responding to Privacy Incidents, Security Incidents, and Breaches.** Each party will comply with this Section for all Protected Information shared under the Agreement. Each party will coordinate and cooperate with one another in responding to and handling any privacy incident, security incident, and/or breach. Additional obligations for specific kinds of Protected Information shared under the Agreement are addressed in subsection 6.2.G, "Reporting Privacy Incidents, Security Incidents, and Breaches."
1. **Mitigation of harmful effects.** Upon discovery of any actual or suspected Privacy Incident, Security Incident, and/or Breach, the Responsible Party will mitigate, to the extent practicable, any harmful effect of the Privacy Incident, Security Incident, and/or Breach. Mitigation may include, but is not limited to, notifying and providing credit monitoring to affected Individuals.
  2. **Investigation.** Upon discovery of any actual or suspected Privacy Incident, Security Incident, and/or Breach, the Responsible Party will investigate to (1) determine the root cause of the incident, (2) identify Individuals affected, (3) determine the specific Protected Information impacted, and (4) comply with notification and reporting provisions of the Agreement, this Agreement, and

---

<sup>2</sup> <https://mn.gov/mnit/government/policies/security/>

applicable law.

3. **Corrective action.** Upon identifying the root cause of any Privacy Incident, Security Incident, and/or Breach, the Responsible Party will take corrective action to prevent, or reduce to the extent practicable, any possibility of recurrence. Corrective action may include, but is not limited to, patching information system security vulnerabilities, sanctioning Agents, and/or revising policies and procedures.
4. **Notification to Individuals and others; costs incurred.**
  - a. **Protected Information.** The Responsible Party will determine whether notice to data subjects and/or any other external parties regarding any Privacy Incident or Security Incident is required by law. If such notice is required, the Responsible Party will fulfill its obligations under any applicable law requiring notification, including, but not limited to, Minnesota Statutes, sections 13.05, "Duties of Responsible Authority," and 13.055, "Disclosure of Breach in Security." If the incident is a "breach of the security of the data," as defined by Minnesota Statutes, section 13.055, the responsible party shall also be responsible for completing the requisite investigation report.
  - b. **Protected Health Information.** If a Privacy Incident or Security Incident results in a Breach of Protected Health Information, as these terms are defined in this Agreement and under HIPAA, then the Responsible Party will provide notice to Individual data subjects under any applicable law requiring notification, including but not limited to providing notice as outlined in 45 C.F.R. § 164.404, "Notification to Individuals."
  - c. **Notification to CMS.** MNsure will serve as the point of contact and notify Centers for Medicare & Medicaid Services (CMS) of incidents related to METS pursuant to the Computer Matching Agreement between CMS and State-Based Administering Entities for the Disclosure of Insurance Affordability Programs Information under the Patient Protection and Affordable Care Act.
  - d. **Notification to OLA.** The Responsible Party shall report any Privacy Incident, Security Incident, and or Breach to the Minnesota Office of Legislative Auditor as required by Minnesota Statutes, section 3.971, subdivision 9.
  - e. **Failure to notify.** If either party incurs costs or is subject to fines or penalties due to the other party's failure to timely and appropriately provide notification under subparagraph (a), then the Responsible Party will reimburse the other party for the costs, fines, or penalties incurred as a result of its failure provide appropriate notification.
5. **Obligation to report to the other party.** Upon discovery of a Privacy Incident, Security Incident, and/or Breach, the Responsible Party will report to the other party in writing as further specified in subsection 6.2.G.
  - a. **Communication with authorized representative.** Each party will send any written reports to, and communicate and coordinate as necessary with, the other party's authorized representative or designee.

- b. **Cooperation of response.** Each party will cooperate with requests and instructions received from the other party regarding activities related to investigation, containment, mitigation, and eradication of conditions that led to, or resulted from, the Security Incident, Privacy Incident, and/or Breach, and all matters pertaining to reporting and notification of a Security Incident, Privacy Incident, and/or Breach.
  - c. **Information to respond to inquiries about an investigation.** Each party will, as soon as possible, but not later than forty-eight (48) hours after a request from the other party, provide the other party with any reports or information requested by the other party related to an investigation of a Security Incident, Privacy Incident, and/or Breach of protected information shared under this agreement.
- 6. **Documentation.** The Responsible Party for the incident or breach will document actions taken under paragraphs 1 through 5 of this subsection, and retain this documentation for a minimum of six (6) years from the date it discovered the Privacy Incident, Security Incident, and/or Breach or the time period required by subsection 6.2.J, whichever is longer. The Responsible Party for the incident or breach shall provide such documentation to the other party upon request.
- G. **Reporting Privacy Incidents, Security Incidents, and Breaches.** Each party will comply with the reporting obligations of this Section as they apply to the kind of Protected Information involved. Each party will also comply with subsection 6.2.F, "Responding to Privacy Incidents, Security Incidents, and Breaches," above in responding to any Privacy Incident, Security Incident, and/or Breach.
  - 1. **Federal Tax Information.** Each party will report all actual or suspected unauthorized Uses or Disclosures of federal tax information (FTI). FTI is information protected by Tax Information Security Guidelines for Federal, State and Local Agencies (26 U.S.C. § 6103 and Publication 1075).
    - a. **Initial report.** Each party will, in writing, immediately report all actual or suspected unauthorized Uses or Disclosures of FTI to the other party. Each party will include in its initial report to the other party all information under subsections 6.2.F(1)–(4), of this Agreement that is available to the party at the time of the initial report, and provide updated reports as additional information becomes available.
    - b. **Final report.** The Responsible Authority will, upon completion of its investigation of and response to any actual or suspected unauthorized Uses or Disclosures of FTI, or upon the other party's request in accordance with subsection 6.2(F)(5), promptly submit a written report to the other party documenting all actions taken under subsections 6.2.F(1)–(4), of this Agreement.
  - 2. **Social Security Administration Data.** Each party will report all actual or suspected unauthorized Uses or Disclosures of Social Security Administration (SSA) data. SSA data is information protected by section 1106 of the Social Security Act.
    - a. **Initial report.** Each party will, in writing, immediately report all actual or suspected unauthorized Uses or Disclosures of SSA data to the other party.

Each party will include in its initial report to the other party all information under subsections 6.2.F(1)–(4), of this Agreement that is available to the party at the time of the initial report, and provide updated reports as additional information becomes available.

- b. **Final report.** The Responsible Party will, upon completion of its investigation of and response to any actual or suspected unauthorized Uses or Disclosures of SSA data, or upon the other party's request in accordance with subsection 6.2.F(5), promptly submit a written report to the other party documenting all actions taken under subsections 6.2.F(1)–(4), of this Agreement.

**3. Protected Health Information.** Each party will report Privacy Incidents, Security Incidents, and/or Breaches involving Protected Health Information as follows:

- a. **Reporting Breaches to DHS.** MNSure will report, in writing, any Breach involving Protected Health Information to DHS within five (5) calendar days of discovery, as defined in 45 C.F.R. § 164.410, "Notification by a Business Associate," subpart (a)(2), for all Breaches involving fewer than 500 Individuals, and immediately for all Breaches involving 500 or more Individuals. These reports shall include, at a minimum, the following information:
  1. Identity of the individuals whose unsecured Protected Health Information has been, or is reasonably believed by MNSure, to have been accessed, acquired, Used, or Disclosed during the incident or Breach.
  2. Description of the compromised Protected Health Information.
  3. Date of the Breach.
  4. Date of the Breach's discovery.
  5. Description of the steps taken to investigate the Breach, mitigate its impact, and prevent future Breaches.
  6. Sanctions imposed on MNSure's Agents involved in the Breach.
  7. All other information that must be included in notification to the Individual under 45 C.F.R. § 164.404(c).
  8. Statement that MNSure has notified, or will notify, impacted Individuals in accordance with 45 C.F.R. § 164.404 and, upon the completion of said notifications, provide through documentation of the recipients, date, content, and manner of the notifications.
- b. **Reporting Breaches to external parties.** The Responsible Party will report all Breaches involving Protected Health Information to the U.S. Department of Health and Human Services (as specified in 45 C.F.R § 164.408, "Notification to the Secretary"), and, for Breaches involving 500 or more Individuals, to the media (as specified in 45 C.F.R. § 164.406, "Notification to the Media"). As soon as possible and no later than 10 (ten) business days prior to any report to the media required by 45 C.F.R. § 164.406, the Responsible Party will provide to the other for its review and approval all Breach-related reports or statements intended for the media.
- c. **Reporting Security Incidents that do not result in a Breach.** Each party will

report, in writing, to the other party all Security Incidents that do not result in a Breach, but involve systems maintaining Protected Health Information shared pursuant to this Agreement within (5) business days of discovery. As a business associate, MNsure and its agents will comply with the applicable requirements of 45 C.F.R. § 164.314, "Organizational Requirements."

- d. **Reporting other violations.** Each party will report, in writing, to the other party any other Privacy Incident and/or violation of an Individual's privacy rights as it pertains to Protected Health Information shared pursuant to this Agreement within five (5) calendar days of discovery as defined in 45 C.F.R. § 164.410(a)(2). This includes, but is not limited to, any violation of Subpart E of 45 C.F.R. Part 164.

**4. Other Protected Information.** Each Responsible Party will report all other Privacy Incidents and/or Security Incidents, to the other party.

- a. **Initial report.** The Responsible Party will report all other Privacy Incidents and/or Security Incidents to the other party, in writing, within five (5) calendar days of discovery. If the Responsible Party is unable to complete its investigation of, and response to, a Privacy Incident, Security Incident, and/or Breach within five (5) calendar days of discovery, then the Responsible Party will provide the other party with all information under subsections 6.2.F(1)–(4), of this Agreement that are available to the Responsible Party at the time of the initial report, and provide updated reports as additional information becomes available.
- b. **Final report.** The Responsible Party will, upon completion of its investigation of and response to a Privacy Incident, Security Incident, and/or Breach, or upon the other party's request in accordance with subsection 6.2.E(5) submit in writing a report to the other party documenting all actions taken under subsections 6.2.F(1)–(4), of this Agreement.

**H. Designated Record Set—Protected Health Information.** If, on behalf of DHS, MNsure maintains a complete or partial designated record set, as defined in 45 C.F.R. § 164.501, "Definitions," upon request by DHS, MNsure shall, in a time and manner that complies with HIPAA or as otherwise directed by DHS:

- 1. Provide the means for an Individual to access, inspect, or receive copies of the Individual's Protected Health Information.
- 2. Provide the means for an Individual to make an amendment to the Individual's Protected Health Information.

**I. Access to Books and Records, Security Audits, and Remediation.** Each party shall conduct and submit to audits and necessary remediation as required by this Section to ensure compliance with all Applicable Safeguards and the terms of the Agreement.

- 1. Each party represents that it has audited and will continue to regularly audit the security of the systems and processes used to provide services under the Agreement, including, as applicable, all data centers and cloud computing or hosting services under contract with a party. Each party will conduct such audits in a manner sufficient to ensure compliance with the security standards referenced in this Agreement.

2. This security audit required above will be documented in a written audit report which will, to the extent permitted by applicable law, be deemed confidential security information and not public data under the Minnesota Government Data Practices Act, Minnesota Statutes, section 13.37, "General Nonpublic Data," subd. 1(a) and 2(a).
3. Each party agrees to make its internal practices, books, audits, and records related to its obligations under the Agreement available to the other party or a designee upon the other party's request for purposes of conducting a financial or security audit, investigation, or assessment, or to determine MNsure's or DHS' compliance with Applicable Safeguards, the terms of this Agreement and accounting standards. For purposes of this provision, other authorized government officials includes, but is not limited to, the Secretary of the United States Department of Health and Human Services.
4. Each party will make and document best efforts to remediate any control deficiencies identified during the course of its own audit(s), or upon request by the other party or other authorized government official(s), in a commercially reasonable timeframe.

**J. Documentation Required.** Any documentation required by this Agreement, or by applicable laws, standards, or policies, of activities including the fulfillment of requirements by a party, or of other matters pertinent to the execution of the Agreement, must be securely maintained and retained by a party for a period of six years from the date of expiration or termination of the Agreement, or longer if required by applicable law, after which the documentation must be disposed of consistent with subsection 6.6 of this Agreement.

Each party shall document Disclosures of Protected Health Information that are subject to the accounting of disclosure requirement described in 45 C.F.R. 164.528, "Accounting of Disclosures of Protected Health Information."

**K. Requests for Disclosure of Protected Information.** If a party or one of its Agents receives a request to Disclose Protected Information, the party shall inform the other party of the request and coordinate the appropriate response with the other party. If a party Discloses Protected Information after coordination of a response with the other party, it shall document the authority used to authorize the Disclosure, the information Disclosed, the name of the receiving party, and the date of Disclosure. All such documentation shall be maintained for the term of the Agreement or six years after the date of the Disclosure, whichever is later, and shall be produced upon demand by the other party.

**L. Conflicting Provisions.** Both parties shall comply with all Applicable Safeguards listed in Section 6.1, including applicable provisions of HIPAA, and with this Agreement. To extent that the parties determine, following consultation, that the terms of this Agreement are less stringent than the Applicable Safeguards, both parties must comply with the Applicable Safeguards. In the event of any conflict in the requirements of the Applicable Safeguards, each party must comply with the most stringent Applicable Safeguard.

**M. Data Availability.** Either party, or any entity with legal control of any Protected

Information provided by the other party, shall make any and all Protected Information under the Agreement available to the other party upon request within a reasonable time as is necessary for the other party to comply with applicable law.

### 6.3 Data Security.

- A. State Information Management System Access.** If a party grants the other party access to Protected Information maintained in a party's information management system (including a "legacy" system) or in any other application, computer, or storage device of any kind, then the party agrees to comply with any additional system- or application-specific requirements as directed by the other party.
- B. Electronic Transmission.** The parties agree to encrypt electronically transmitted Protected Information in a manner that complies with NIST Special Publications 800-52, "Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations"; 800-77, "Guide to IPsec VPNs"; 800-113, "Guide to SSL VPNs," or other methods validated under Federal Information Processing Standards (FIPS) 140-2, "Security Requirements for Cryptographic Modules." As part of its compliance with the NIST publications, and the State of Minnesota's "Enterprise Information Security Policies and Standards,"
- C. Portable Media and Devices.** The parties agree to encrypt Protected Information written to or stored on portable electronic media or computing devices in a manner that complies with NIST SP 800-111, "Guide to Storage Encryption Technologies for End User Devices."

### 6.4 MNsure Permitted Uses and Responsibilities regarding Protected Health Information.

- A. Management and Administration.** Except as otherwise limited in the Agreement, MNsure may:
  - 1. Use Protected Health Information for the proper management and administration of MNsure or to carry out the legal responsibilities of MNsure.
  - 2. Disclose Protected Health Information for the proper management and administration of MNsure, provided that:
    - a. The Disclosure is required by law; or
    - b. The Disclosure is required to perform the services provided to or on behalf of DHS or the Disclosure is otherwise authorized by DHS, and MNsure:
      - i. Obtains reasonable assurances from the entity to whom the Protected Health Information will be Disclosed that the Protected Health Information will remain confidential and Used or further Disclosed only as required by law or for the purposes for which it was Disclosed to the entity; and
      - ii. Requires the entity to whom Protected Health Information is Disclosed to notify MNsure of any instances of which it is aware in which the confidentiality of Protected Health Information has been Breached or otherwise compromised.
- B. Notice of Privacy Practices.** If MNsure's duties and responsibilities require it, on behalf of DHS, to obtain individually identifiable health information from Individual(s), then



MNsure shall, before obtaining the information, confer with DHS to ensure that any required Notice of Privacy Practices includes the appropriate terms and provisions.

- C. De-identify Protected Health Information.** MNsure may use Protected Health Information to create de-identified Protected Health Information provided that MNsure complies with the de-identification methods specified in 45 C.F.R. § 164.514, "Other Requirements Relating to Uses and Disclosures of Protected Health Information." De-identified Protected Health Information remains the sole property of DHS and can only be Used or Disclosed by MNsure on behalf of DHS and pursuant to the Agreement or by prior written approval of DHS.
- D. Aggregate Protected Health Information.** MNsure may use Protected Health Information to perform data aggregation services for DHS, and any such aggregated data remains the sole property of DHS. MNsure must have the written approval of DHS prior to using Protected Health Information to perform data analysis or aggregation for parties other than DHS.

## **6.5 DHS Permitted Uses and Responsibilities regarding Protected Information**

- A. Management and Administration.** Except as otherwise limited in this Agreement, DHS may:
  - 1. Use Protected Information for the proper management and administration of DHS or on behalf of MNsure or to carry out the legal responsibilities of MNsure or DHS, provided that any access to data classified as not public data under Minnesota Statutes, section 62V.06, subd. 3, by individual agents of DHS is approved by the MNsure Board pursuant to Minnesota Statutes, section 62V.06, subd. 8.
  - 2. Disclose Protected Information for the proper management and administration of DHS or on behalf of MNsure, provided that:
    - a. The disclosure is required by law; or
    - b. The disclosure is required to perform the services provided to or on behalf of MNsure or the disclosure is otherwise authorized by MNsure, and DHS:
      - i. Obtains reasonable assurances, in the form of a data sharing agreement, from the entity to whom the Protected Information will be disclosed that the Protected Information will be safeguarded in accordance with law and will not be used or disclosed other than for the contracted services or the authorized purposes; and
      - ii. DHS requires the entity to whom Protected Information is disclosed to notify DHS of any compromise to the confidentiality, availability, and integrity of Protected Information of which it becomes aware.
- B. Sale of Data Prohibited.** The parties are prohibited from selling any data that is classified by Minnesota Statutes, section 62V.06.

## **6.6 Obligations Upon Expiration or Cancellation of the Agreement.** Upon expiration or termination

of the Agreement for any reason:

- A. In compliance with the procedures found in the Applicable Safeguards listed in subsection 6.1.A, or as otherwise required by applicable industry standards, or directed by the other party, each party shall immediately destroy or sanitize (permanently de-identify without the possibility of re-identification), or return in a secure manner to the other party all Protected Information that it still maintains.
- B. Each party shall ensure and document that the same action is taken for all Protected Information shared by the other party that may be in the possession of its Agents. Each party and its Agents shall not retain copies of any Protected Information of the other party.
- C. In the event that a party determines that returning or destroying the Protected Information is not feasible or would interfere with its ability to carry out its legal responsibilities, maintain appropriate safeguards, and/or comply with Subpart C of 45 C.F.R. Part 164, it shall notify the other party of the specific laws, rules, policies, or other circumstances that make return or destruction not feasible or otherwise inadvisable. Upon mutual agreement of the Parties that return or destruction of Protected Information is not feasible or otherwise inadvisable, the party will continue to extend the protections of the Agreement to the Protected Information and take all measures possible to limit further Uses and Disclosures of the Protected Information for so long as it is maintained by the party or its Agents.
- D. Each party shall document and verify in a written report to the other party the disposition of Protected Information. The report shall include at a minimum the following information:
  - 1. A description of all Protected Information that has been sanitized or destroyed, whether performed internally or by a service provider;
  - 2. The method by which, and the date when, the Protected Data were destroyed, sanitized, or securely returned to the other party; and
  - 3. The identity of organization name (if different than the party), and name, address, and phone number, and signature of Individual, that performed the activities required by this Section.
- E. Documentation required by this Section shall be made available upon demand by the other party.
- F. Any costs incurred by a party in fulfilling its obligations under this Section will be the sole responsibility of the party.

**7. LIABILITY.**

The parties agree that each is independently responsible for complying with statutes, rules, and regulations governing or affecting the collection, storage, use, sharing, disclosure, and dissemination of Protected Information in accordance with Clause 6 Information Privacy and Security. Neither party will be liable for any violation of any provision of applicable laws or the terms of this Agreement indirectly or directly arising out of, resulting from, or in any manner attributable to actions of the other party or its employees or agents. The liability of each party is governed by the provisions of the Minnesota Tort Claims Act, Minnesota Statutes, section 3.736, and other applicable law.

The parties acknowledge that if a party is in violation of this Agreement, or violation of a federal or state statute applicable to Protected Information, the other party may limit, suspend, or terminate the violating party's access to or use of Protected Information.

**8. SEVERABILITY.**

If any provision of this Agreement is held unenforceable, then such provision will be modified to reflect the parties' intention. All remaining provisions of this Agreement shall remain in full force and effect.

**9. INTERPRETATION**

Any ambiguity in this Agreement shall be interpreted to permit compliance with all Applicable Safeguards.

**10. SURVIVAL OF TERMS.**

The rights and obligations of the parties under this Agreement shall survive the termination of this Agreement for as long as each party or its subcontractors and agents are in possession of Protected Information received from or collected, created, used, maintained, or disclosed on behalf of the other party. The duties and obligations of both parties in section 6.6 shall survive termination of this Agreement.

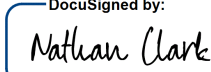
**REMAINDER OF PAGE INTENTIONALLY LEFT BLANK.**

By signing below, the parties agree to the terms and conditions contained in this AGREEMENT.


**APPROVED:**

**1. MNSURE**

*MNSURE certifies that the appropriate person(s) have executed the Agreement on behalf of MNSURE as required by applicable articles, by-laws resolutions or ordinances.*

By: Click here to enter text   
Printed Name: Nathan Clark 60CA7E6941CA4DB...  
Title: Chief Executive Officer  
Date: Click here to enter text 12/31/2020

**2. Department of Human Services (DHS)**

By (with delegated authority): Click here to enter text   
Printed Name: Click here to enter text Charles E. Johnson E336517A7B0D415...  
Title: Click here to enter text Deputy Commissioner  
Date: Click here to enter text 12/31/2020

**Distribution: (copy of fully executed contract to each)**

Contracting and Legal Compliance Division

MNsure

DHS Authorized Representative

# Amendment No.1 to Interagency Agreement 201592

Contract Start Date:	October 14, 2021	Original Contract:	\$13,073,259
Original Contract Expiration Date:	<u>6/30/2023</u>	Previous Amendment(s) Total:	<u>\$0</u>
Current Contract Expiration Date:	<u>6/30/2023</u>	This Amendment:	<u>\$0</u>
Requested Contract Expiration Date:	<u>N/A</u>	Total Contract Amount:	<u>\$13,073,259</u>

**This amendment** ("Amendment") is by and between Minnesota Department of Human Services, Commissioner's Office Division, (hereinafter DHS) and the Chief Executive Officer of the Minnesota Health Insurance Marketplace (hereinafter "MNSure").

## Recitals

1. DHS and MNSure have an agreement identified as IAK-201592 ("Original Agreement") to allow DHS to provide standard, centralized administrative services to MNSure;
2. DHS and MNSure agree that the Original Agreement should be modified in order to add services for proof of vaccination and testing as described in Revised Exhibit B;
3. DHS and MNSure are correcting a typographical error in Section 3.1; and
4. DHS and MNSure are willing to amend the Original Agreement as stated below.

## Contract Amendment #1

In this Amendment, changes to Original Agreement language will use ~~strike through~~ for deletions and underlining for insertions.

The parties agree to the following revisions:

### REVISION 1. Clause 1.1 "Human Resources" is amended as follows:

- 1.1 Human Resources.** DHS shall provide human resource services to MNSure in accordance with the duties, responsibilities, and obligations set forth in Revised Exhibit B, which are attached and incorporated into this Agreement.
  - A. Scope of Work.** MNSure shall retain ownership and responsibility for its human resource decisions, while DHS shall serve in an advisory capacity and provide transaction and other services. MNSure shall be responsible for paying all costs associated with all independent investigations.

**B. Authorized Representatives.**

1. DHS' authorized representative in regards to human resource services is Connie Jones, Human Resources Director, or her successor.
2. MNSure's authorized representative in regards to human resource services is Dave Rowley, General Counsel, or his successor.
3. Each representative shall have final authority for acceptance of human resource services of the other party and shall have responsibility to ensure that all payments due to the other party with respect to human resource services are made pursuant to the terms of this Agreement.

**REVISION 2. Clause 3.1 "Scope of Work" is amended as follows:**

**3.1 Scope of Work.** Payments made and invoices submitted between DHS and MNSure under Section 1 and Section ~~2~~ 2.1 of this Agreement are based on direct costs, including the associated Full Time Employee (FTE) positions. This Section addresses the occupancy and IT support indirect costs attributable to these FTE positions. DHS may submit, and MNSure shall pay, invoices for occupancy and IT support indirect costs associated with FTE assigned to perform work under this Agreement.

**EXCEPT AS AMENDED HEREIN, THE TERMS AND CONDITIONS OF THE ORIGINAL AGREEMENT AND ALL PREVIOUS AMENDMENTS REMAIN IN FULL FORCE AND EFFECT AND ARE INCORPORATED INTO THIS AMENDMENT BY REFERENCE.**

***REMAINDER OF PAGE INTENTIONALLY LEFT BLANK  
SIGNATURE PAGE FOLLOWS***

### **REVISED EXHIBIT B - Human Resource Services**

DHS will provide the agency the following human resource services that will help MNsure operate effectively:

#### Transactions

- Complete accurate and timely SEMA-4 changes related to changes in employee information, hire, funding; promotion, separation dates, increase dates, department ID, medical leaves of absence, performance reviews, etc.
- Seniority Rosters will be updated/posted as required by contracts/plans.

Timely transactions depend on DHS receiving timely information from MNsure about employee status. DHS is not responsible for processing information if it has not received a written request.

#### ***Performance Management***

Definition: Developing standards and policies and providing support for supervisors and managers to provide constructive and developmental feedback and direction for 'ongoing coaching as well as a context for management decision-making.

- Train management on performance improvement techniques.
- Advise managers and supervisors in investigating employee misconduct, performance or attendance problems, or recommend retention of an outside Investigator. Investigations for managerial staff will be referred to an independent Investigator outside the state. DHS will coordinate the investigation.
- Advise managers and supervisors on handling performance, attendance, and conduct issues with employees.
- Assist managers and supervisors in withholding performance increases, taking disciplinary action, or discharging employees.
- Draft disciplinary letters and letters of expectations.
- Advise managers and supervisors on human resources best practices in employee motivation, reviews, and supervisory practices.

MNsure is responsible for paying all costs associated with independent investigations.

#### ***Human Resources Policy Management***

Definition: Researching, developing, recommending, implementing, and communicating an array of Human Resources policies to support consistent employment practices.

- Investigate the need for and write new policies for human resource issues.
- Maintain and update existing policies.

#### Contract Administration

- Advise managers and supervisors on the proper application of contract language. When appropriate, DHS will seek MMB's advice on contract interpretation.
- Advise managers and supervisors on the practical application of employment laws such as FMLA, FLSA, ADA, USERRA, and all discrimination laws.

#### ***Training***

Definition: Providing strategy, planning, and implementation of targeted learning activities to support both individual employee development and organizational strategies. This training is restricted to employees of MNSure.

- In conjunction with MNSure HR Specialist, train managers and supervisors on human resources practices, employment law, bargaining unit contract language/ compensation, code of ethics, and other topics directly related to human resources.

#### ***Classification and Compensation***

Definition: Conduct an analysis of the individual position to identify and describe the different kinds of work in an organization and group similar positions under common classification titles based upon the kind of work, degree of difficulty and the, responsibilities required.

- Review position descriptions; determine appropriate classification, document audit decisions, and explain the rationale for classification decisions.
- Coordinate Hay sessions when applicable.
- Conduct studies of groups of positions as necessary.
- Approve or deny compensation requests for new hires or promotions.
- Supervisors will receive notification of positions that are ending each quarter.

MNSure must provide documentation of requests to convert unclassified position to the classified service at least one month in advance of the end of the unclassified position.

DHS has received delegated authority from MMB-Enterprise Human Resources to make classification and compensation decisions. DHS must abide by accepted practices and rules governing classification and compensation in order to retain this delegation. MMB-Enterprise Human Resources periodically audits DHS's work to determine compliance with rules and laws.

#### ***Vacancy-Filling***



Definition: Work With HR Specialist who works directly to assist managers in hiring so that MNsure follows state bargaining unit contracts, employment laws, and state laws governing state positions. This includes filling vacancies by developing appropriate qualifications for vacancies, determining recruitment options, posting, reviewing candidates resumes to determine qualified candidates, and assisting the supervisor or managers in following state bargaining unit contracts and state laws.

- Advise on minimum qualifications and recruitment options.
- Posting and bidding/expression of interest process for classified positions.
- Review position applications to determine which applicants meet the minimum qualifications and refer successful candidates to the hiring supervisor.
- Assist managers and supervisors in developing interview questions and other selection criteria and exercises.
- Conduct background checks.
- Document hires for affirmative action purposes.
- Compose offer and employment confirmation letters.
- Notify all applicants of position hiring decisions.
- Close out Resumix

### ***Labor Relations and Employment Law***

Definition: Ongoing maintenance and development of union and employee relations in order to advise management on performance and employment law issues, standards; and policies.

- Represent management at meet and confer sessions.
- Respond to third-step grievances for MNsure.
- Review and responding to requests for accommodation under the ADA.
- Monitor payroll and leave under USERRA.
- Notify MNsure of new laws, state rules, and issues.
- Investigate all significant workers' compensation claims, process claims, and work through settlements and resolutions on behalf of MNsure.
- Advise supervisors and managers with other employment law issues such as discrimination, sexual harassment, etc.

- Review unemployment claims and represent management in unemployment hearings.

### ***Safety & Workers' Compensation***

- File yearly OSHA lost-time reports.
- Assist with first reports of injury filings.

### ***Reporting***

- Upon request, provide ad hoc reports on employee costs, leave use, hires, separations, and other employment Information contained in the state's information warehouse.

### ***File Maintenance & Storage***

- Maintain and store audit (Job classification decision) files and requisitions (vacancy filling) files.
- Inform MNSure on the types of personnel information that should be securely maintained onsite.
- Maintain Personnel files/records.

### **Proof of Vaccination and Testing**

- DHS will coordinate vaccine attestation, testing consent, and other required medical documentation on behalf of MNSure for vaccine attestation or testing required by State policy, including but not limited to HR/LR Policy # 1446 (COVID-19 Proof of Vaccination and Testing).
- DHS will purchase and track test kits, including but not limited to COVID-19 test kits, on MNSure's behalf. DHS will provide MNSure with weekly updates on the status of the test results and attestation status.
- DHS will not seek reimbursement from MNSure for the test kits unless DHS is unable to obtain reimbursement for the full costs of the test kits from the Federal government. MNSure shall reimburse DHS for test kit costs that are not covered by Federal government reimbursement.
- DHS will distribute test kits to MNSure's employees as needed and consistent with State policy, and check the results of the tests with the designated vendor.

### **DHS Human Resources Responsibilities:**

DHS will provide the following level of service:

- Vacancies will be posted within two business days of receipt of a request to fill (if the position does not need to be allocated or the allocation changed)
- Examine 1-9 documentation, after hire, for legal hiring.

- Positions requiring initial allocation will be allocated within two weeks of the receipt of a complete position description, organizational chart, and request memo.
- Positions requiring reallocation will be audited within four to six weeks of the receipt of a complete position description, organizational chart, and request memo.
- Investigations will be conducted promptly. Timing depends on the exact circumstances and availability of union representatives.
- Transactions turned In by Thursday of the non-payroll week will take effect that payroll period.
- Employees hired during the last two days of the pay period may not be paid for those days until the next pay period.

#### **MNsure's Responsibilities:**

Management of MNsure is responsible for the actions of the organization's employees, including unethical, violent, or harassing behavior and failure to follow state policies and procedures.

MNsure is responsible for completing the following human resource actions:

#### ***Benefits Administration***

- Convey benefits information from Minnesota Management and Budget (DHS) to employees of MNsure.
- Benefits questions and issues will be handled directly by the State Employee Group Insurance Program (SEGIP) at MMB. All employees will receive information on the SEGIP contact.
- FMLA requests: All employees will receive information on how to apply for FMLA from DHS and supervisors and managers will coordinate directly with DHS.

#### ***Training***

Definition: Providing strategy, planning, and Implementation of targeted learning activities to support both individual employee development and organizational strategies. This training is restricted to employees of MNsure.

- In conjunction with DHS, train managers and supervisors on human resources practices, employment law, bargaining unit contract language, compensation, code of ethics, and other topics directly related to human resources.
- Track completion on topics mandated by law or policy - code of conduct, sexual harassment prevention, right-to-know, etc.
- Send communications to employees about various human resource topics.

#### ***Policies and Procedures***

- MNsure has appointed an Ethics Officer and communicated that designation to employees.

- Employees are trained on the Code of Ethics (M.S. 43A.18) and as required the Code of Conduct.
- Position descriptions clearly indicate the employee's level of decision-making authority.
- Employees receive copies of general statewide policies and policies and procedures governing their particular jobs.
- Formal delegations of duties are on file.
- Operating practices are consistent with state policies.
- Appropriate action is taken for violations of policy.

#### ***Position Descriptions***

- All positions have position descriptions that are updated at least every three years.
- Position descriptions are consistent with employees' actual job duties and include a listing of essential functions under the ADA.

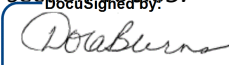
#### ***Employee Performance Management***

- New employees must receive copies of their position descriptions and an orientation to their work and their work unit,
- All new employees must receive mid-probationary and probationary reviews.
- All employees must be given honest feedback on their performance at least once a year with a written formal evaluation placed in their personnel
- Performance expectations are made clear for all employees.
- Employees whose performance, attendance, or behavior is problematic will be coached on their deficiencies to permit them to improve- unless the behavior is so severe that immediate action must be taken to end their appointment. All such issues should be discussed with the DHS Labor Relations Representative.

**APPROVED:**

**1. STATE ENCUMBRANCE VERIFICATION**

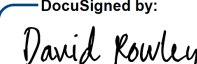
*Individual certifies that funds have been encumbered as required by Minnesota Statutes, chapter 16A and section 16C.05.*

By:   
5457B11AE8BB49D...

Date: 12/30/2021

SWIFT Contract No: IAK 201592

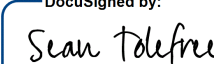
**2. MNsure**

By with delegated authority):   
EC8826518E5C4F5...

Title: General Counsel

Date: 12/30/2021

**3. MN Department of Human Services**

By (with delegated authority):   
379F70C21CF04BB...

Title: HR Director

Date: 12/30/2021



---

# Comprehensive IT FY22-23 Service Level Agreement

In direct support of  
MNsured Business Operations

07/01/2022

---

## Table of Contents

---

Table of Contents	2
<b>Section 1: Service Agreement – General Terms</b>	<b>12</b>
Introduction	12
Objectives	13
Review Process	13
Common Partnership	14
MNIT Roles and Responsibilities	14
The Agency Roles and Responsibilities	16
The Chief Business Technology Officer Roles and Responsibilities	17
Data Handling Roles and Responsibilities	18
Budget Scope	19
Acceptance	19
Dispute Management	20
Liability	20
Additional Provisions	20
Law to Govern	20
Assignment	21
<b>Section 2: Service Agreement – Projects and Services</b>	<b>22</b>
Projects	22
Services	23
1. Enterprise Services*	23
2. Shared Services*	23
3. Center of Excellence Services	23
4. Local Services	23
5. Enterprise Security Services*	23
Center of Excellence Services Summary	24
Local Services Summary <i>For detail, please refer to Local Services description(s) in Section 2</i>	24
Enterprise Security Services Summary <i>For detail, please refer to the Enterprise Security Services description in Section 2</i>	24

<b>Service Name: Database Support - Shared Services</b>	<b>25</b>
Revision Date 10/28/2021	25
Executive Summary	25
Description	25
What systems or services are supported?	26
Distributed systems supported database management software	26
Mainframe supported database management software	26
What services are included?	26
What services are NOT included?	27
Dedicated Hosted Database Support does not include:	27
How will the service be delivered?	27
What are the hours of operation and how to get support?	27
What will the response time be?	28
What are the business responsibilities?	29
When will regular maintenance be performed?	29
Change Management Process/Termination	29
<b>Service Name: Enterprise Hosting</b>	<b>30</b>
Revision Date 10/18/2021	30
Executive Summary	30
Description	30
What systems or services are supported?	31
What services are included?	31
What services are NOT included?	32
How will the service be delivered?	32
What are the hours of operation and how to get support?	32
What will the response time be?	33
What are the business responsibilities?	33
When will regular maintenance be performed?	34
Change Management Process/Termination	34
<b>Service Name: Local Area Network (LAN) Services</b>	<b>34</b>



Revision Date 09/01/2021	34
Executive Summary	34
Description	35
What systems or services are supported?	35
What services are included?	35
What services are NOT included?	35
How will the service be delivered?	35
What are the hours of operation and how to get support?	36
Minnesota IT Services Service Desk Contacts	36
What will the response time be?	37
What are the business responsibilities?	37
When will regular maintenance be performed?	38
Change Management Process/Termination	38
<b>Service Name: Middleware Support - Shared Services</b>	<b>39</b>
Revision Date 09/15/2021	39
Executive Summary	39
Description	39
What systems or services are supported?	39
Distributed systems supported software	39
Mainframe supported software	40
What services are included?	40
What services are NOT included?	40
How will the service be delivered?	41
What are the hours of operation and how to get support?	41
What is the response time?	42
What are the business responsibilities?	43
When will regular maintenance be performed?	43
Change Management Process/Termination	43
<b>Service Name: Minnesota Enterprise Identity and Access Management (MNEIAM)</b>	<b>44</b>
Revision Date 02/10/2022	44

Executive Summary	44
Description	45
What systems or services are supported?	45
What services are included?	45
What services are NOT included?	45
How will the service be delivered?	45
What are the hours of operation and how to get support?	45
What will the response time be?	46
What are the business responsibilities?	47
When will regular maintenance be performed?	48
Change Management Process/Termination	48
<b>Service Name: Web Management Services</b>	<b>49</b>
Revision Date 09/15/2021	49
Executive Summary	49
Description	49
What systems or services are supported?	50
What services are included?	50
What services are NOT included?	50
How will the service be delivered?	51
What are the hours of operation and how to get support?	51
What will the response time be?	52
What are the business responsibilities?	53
When will regular maintenance be performed?	53
Change Management Process/Termination	53
<b>Service Name: Laptop/Desktop Bundle</b>	<b>54</b>
Revision Date 07/14/2021	54
Executive Summary	54
Description	54
Considerations	55
What systems or services are supported?	55

What services are included?	55
What services are NOT included?	55
How will the service be delivered?	56
What are the hours of operation and how to get support?	56
What will the response time be?	57
What are the business responsibilities?	57
When will regular maintenance be performed?	58
Lost, stolen or damaged equipment caused by negligence	58
Change Management Process/Termination	58
<b>Service Name: Enterprise Security Services</b>	<b>59</b>
Revision Date 09/14/2021	59
Executive Summary	59
Enterprise Threat and Vulnerability Management	60
Security Operations Center (SOC)	61
Digital Forensics	62
Secure Engineering and Architecture	63
Enterprise Privileged Account Management Service	64
Enterprise Digital Certificate and Encryption Key Management (PKI)	65
Enterprise Governance, Risk, and Compliance	66
Description	67
Enterprise Threat and Vulnerability Management	67
Security Operations Center	67
Digital Forensics	67
Secure Engineering and Architecture	67
Secure Engineering and Architecture (SEA), a function of Enterprise Architecture, proactively engages IT engineers, architects and developers to design security controls into IT systems and applications early in the development lifecycle. The focus of SEA is to ensure purchased, outsourced, or internally developed IT systems and applications are designed and implemented to meet the State of Minnesota's security architecture and secure coding standards.	67
Enterprise Privileged Account Management Service	68
Enterprise Digital Certificate and Encryption Key Management (PKI) Service	68
Enterprise Governance, Risk and Compliance	68

What systems or services are supported?	69
Security Operations Center and Digital Forensics	69
Privileged Account Management Service	69
Enterprise Digital Certificate and Encryption Key Management (PKI) Service	69
What services are included?	70
Enterprise Threat and Vulnerability Management	70
Security Operations Center	70
Digital Forensics	71
Privileged Account Management Service	71
Enterprise Digital Certificate and Encryption Key Management (PKI) Service	71
What services are NOT included?	71
Enterprise Threat and Vulnerability Management	71
Security Operations Center	72
Digital Forensics	72
Privileged Account Management Service	72
Enterprise Digital Certificate and Encryption Key Management (PKI) Service	72
How will the service be delivered?	72
What are the hours of operation and how to get support?	72
What are the business responsibilities?	73
Privileged Account Management Services	73
Enterprise Digital Certificate and Encryption Key Management (PKI) Service	73
When will regular maintenance be performed?	73
Change Management Process/Termination	73
<b>Service Name: Enterprise Software Bundles</b>	<b>74</b>
Revision Date 07/15/2021	74
Executive Summary	74
Description	75
What systems or services are supported?	75
Workstation Services and Rates (Core Service)	75
Kiosk Worker Services and Rates (Core Service)	76

Exchange only	76
What services are included?	76
What services are NOT included?	76
How will the service be delivered?	76
What are the hours of operation and how to get support?	77
<b>Minnesota IT Services Service Desk Contacts</b>	77
What will the response time be?	77
What are the business responsibilities?	78
When will regular maintenance be performed?	78
Change Management Process/Termination	78
<b>Service Name: Geospatial Shared Services</b>	<b>79</b>
Revision Date 10/28/21	79
Executive Summary	79
What systems or services are supported?	80
What services are included?	80
Enterprise Licensing for GIS Software	80
Minnesota Geospatial Commons	80
Web Services	80
Geospatial Managed Hosting	81
Professional Services	81
Contact us for more Information	81
How will the service be delivered?	81
What are the hours of operation and how to get support?	81
What will the response time be?	82
What are the business responsibilities?	83
When will regular maintenance be performed?	83
Change Management Process/Termination	83
<b>Service Name: Voice</b>	<b>84</b>
Revision Date 09/01/2021	84
Executive Summary	84

Description	84
What systems or services are supported?	84
What services are included?	84
What services are NOT included?	85
How will the service be delivered?	85
What are the hours of operation and how to get support?	86
MNIT Service Desk Contacts	86
What will the response time be?	87
What are the business responsibilities?	88
When will regular maintenance be performed?	88
Change Management Process/Termination	89
<b>Service Name: Wide Area Network (WAN) Services</b>	<b>89</b>
Revision Date 09/01/2021	89
Executive Summary	89
Description	89
What systems or services are supported?	90
What services are included?	90
What services are NOT included?	90
How will the service be delivered?	90
What are the hours of operation and how to get support?	92
<b>MNIT Service Desk Contacts</b>	92
What will the response time be?	93
What are the business responsibilities?	93
When will regular maintenance be performed?	94
Change Management Process/Termination	94
<b>Mobile Device Management/MNIT Enterprise Services</b>	<b>95</b>
Revision Date 09/30/2021	95
Executive Summary	95
Description	96
Service Delivery Method	96

What are the hours of operation and how to get support?	97
What will the response time be?	97
What are the business responsibilities?	98
When will regular maintenance be performed?	98
Lost, stolen or damaged equipment caused by negligence	98
Change Management Process/Termination	98
<b>Service Name: Salesforce Development &amp; Support (SFDC) – Center of Excellence</b>	<b>99</b>
Revision Date 08/27/2018	99
Executive Summary	99
Description	99
What systems or services are supported?	99
What services are included?	99
What services are NOT included?	100
How will the service be delivered?	100
What are the hours of operation and how to get support?	100
What will the response time be?	101
What are the business responsibilities?	102
When will regular maintenance be performed?	102
Change Management Process/Termination	102
<b>Local Services Summary</b>	<b>103</b>
Revision Date 01/12/2022	103
Description	103
What systems or services are supported?	103
What services are included?	103
What services are NOT included?	105
How will the service be delivered?	105
What are the hours of operation and how to get support?	105
What will the response time be?	106
What are the business responsibilities?	106
When will regular maintenance be performed?	107

Change Management Process/Termination	107
<b>Service Name: Mainframe</b>	<b>108</b>
Executive Summary	108
Description	108
What systems or services are supported?	108
What services are included?	109
What services are NOT included?	109
How will the service be delivered?	109
What are the hours of operation and how to get support?	109
What will the response time be?	110
What are the business responsibilities?	110
When will regular maintenance be performed?	111
Change Management Process/Termination	111
<b>Section 3: Service Agreement – Performance Metrics</b>	<b>112</b>
Performance Metrics	112
1. Security Performance Reports/Metrics:	112
2. Enterprise Services Incident and Response Metrics:	112
<b><i>Open Enrollment Support Agreement between MNSure and MNIT Partnering with the Department of Human Services and MNSure</i></b>	<b>113</b>
<b>Scope and Purpose</b>	<b>114</b>
Revision History	115
<b>MNIT Support Hours</b>	<b>116</b>
MNIT@DHS/MNSure Service Desk (Tier 2) Core Hours	116
Tier 2 Core Hours during Open Enrollment	116
MNIT Support Outside of Core Hours	116
Changes to Support Hours during Open Enrollment	116
MNIT Enterprise Service Desk (ESD)	116
<b>MNIT and MNSure Contact Information</b>	<b>117</b>
MNIT Contact Information	117
MNIT Enterprise Service Desk	118



MNsure Contact Information	119
<b>Incident Management Processes</b>	<b>120</b>
Incident Reporting	120
Incident Response	120
Incident Investigation and Mitigation	122
Incident Status Reporting	123
<b>Terms and Definitions</b>	<b>124</b>
<b>Signature Page</b>	<b>126</b>

# Section 1: Service Agreement – General Terms

## Introduction

---

The purpose of this Service Level Agreement (SLA) is to provide a basis for close cooperation between Minnesota IT Services (MNIT) and agencies, boards, and councils (Agency) and for support services to be provided by MNIT to the Agency, thereby ensuring that IT services are timely, cost effective, and efficient for the Agency.

The complete agreement consists of four sections:

- 1. Service Agreement: General Terms
- 2. Service Agreement: Projects and Services
- 3. Service Agreement: Performance Metrics
- 4. Open Enrollment Support Agreement between MNsure and MNIT Partnering with the Department of Human Services and MNsure

The primary objective of this SLA is to define the service delivery items that will govern the relationship between MNIT and the Agency. This SLA documents the required business-facing information technology (IT) services that support the existing Agency business processes at the existing service levels.

This SLA, and all supporting documents which are incorporated herein by reference, supersedes in its entirety any previous service level agreements between MNIT and the Agency, or any other similar agreements relating to Laws of Minnesota 2011, First Special Session chapter 10, article 4 (the IT Consolidation Act). This SLA is authorized by and implements the requirements set forth in the IT Consolidation Act.

For purposes of this SLA, “information technology” (IT) is defined as the acquisition, storage, communication, and processing of information by computers, telecommunications, applications and other software. This includes, but is not limited to: business data, voice, images, and video. IT provides an agency with business process automation, productivity tools and information delivery services to help execute the business strategy. Specific components of IT include, but are not limited to, enterprise-wide and agency-specific applications (business application software and related technical support services), system software, networks, databases, telecommunications, data centers, mainframes, servers, desktops, laptops/mobile computing devices, output devices such as printers, electronic mail, office systems, reporting, and other standard software tools, help desk, upgrades, security and IT service continuity, and maintenance and support of these systems.

The success of this SLA and the cooperative relationship created is dependent on each party understanding and fulfilling their responsibilities and generating an environment conducive to the achievement and maintenance of targeted service levels.

## Objectives

---

- To create an environment that is conducive to a cooperative relationship between MNIT and the Agency to ensure the effective support of the Agency as it conducts its business.
- To document the roles and responsibilities of all parties taking part in the SLA.
- To ensure that the Agency receives the provision of agreed upon service levels with the support of MNIT.
- To define the services to be delivered by MNIT and the level of expected service and anticipated costs that can be expected by the Agency, thereby reducing the possibility for misunderstandings.
- To provide a common understanding of service requirements or capabilities and service levels and objectives.
- To provide a single, easily referenced document that addresses the objectives as listed above.

## Review Process

---

This SLA will be reviewed by MNIT and the Agency no less frequently than every two years. MNIT and the Agency will maintain regular dialog and use the SLA as a basis for cooperation between the two entities in order to ensure that the Agency is receiving the services it needs.

## Common Partnership

---

MNIT and the Agency will work collaboratively to meet the State's strategic direction and business needs and will establish a cooperative relationship to achieve efficiencies and improve the delivery of technology services.

MNIT and the Agency agree to all terms in this Agreement, including as follows:

- In conjunction with state agencies and other stakeholders, MNIT will establish and maintain a formal governance process that includes agency business participation and incorporates agency business requirements into overall IT strategy and direction.
- MNIT's oversight authority includes IT planning activities, IT budget management, IT purchasing, IT policy development and implementation, and direction of MNIT employees. MNIT's oversight authority does not extend to the non-IT portions of the Agency's business operations, plans or needs.
- MNIT provides enterprise IT services to all state agencies, boards, and councils as defined in Minnesota Statutes, Chapter 16E. MNIT assigns a Chief Business Technology Officer (CBTO) to work with agencies, boards, and councils to deliver and sustain agency-specific solutions to meet their unique mission, system and application requirements.
- In collaboration with Agency, MNIT is responsible for the accounting, management, and inventory of any IT property and assets purchased by MNIT post-consolidation for the purpose of compliance with statewide property management and accounting policies and procedures. The Agency is responsible for any IT property or assets purchased pre-consolidation. MNIT is dependent upon Agency to assist with the IT property and asset management and inventory. The Agency is responsible to utilize inventory best practices such as, but not limited to, submitting timely offboarding tickets, reporting lost, stolen or unused equipment, sharing federal asset purchasing requirements with MNIT, and other actions that impact MNIT's ability to account for, manage, and inventory IT property and assets.

## MNIT Roles and Responsibilities

---

MNIT will work with the Agency to ensure the best interest of the state and the Agency it supports.

MNIT has the responsibility to:

- Coordinate, develop, communicate, and manage all IT strategic planning and establish the state's IT direction in the form of policies, standards, guidelines and directives.
- Collaborate with agencies to develop and determine delivery strategies for all executive branch state agency IT activity and services consistent with the IT Governance Framework.

- Manage IT resources at the executive branch level based on strategic planning, service delivery strategies, Agency and executive branch business needs, and legal requirements pertaining to IT resources and IT resource funding.
- Report regularly to agencies on service delivery performance and timelines and get feedback from agencies on service levels and business needs.
- Manage all IT employees. All IT employees are MNIT employees and report through the MNIT Commissioner.
- Perform human resources services for MNIT employees. MNIT Human Resources (HR) has authority to perform IT-related employment tasks including, but not limited to, transactions, classification, compensation, staffing (including hiring and termination), labor relations, unemployment, workforce planning, recruitment, training, safety and investigations (those items subject to delegation by Minnesota Management and Budget are to the extent delegated by Minnesota Management and Budget). MNIT will consult with Agency if/when making Agency-based CBTO hiring decisions.
- Work with agencies to support development of legislative initiatives related to IT.
- Determine responsibility, role and compensation for the Agency-based CBTO. Create a position description, complete performance appraisals of the Agency-based CBTO and obtain performance feedback from Agency, and implement performance-related measures, including performance management.
- Implement and maintain appropriate IT internal controls for all IT-related business needs. Additionally, set information security policies and standards, and oversee the security of the state's executive branch information and telecommunications technology systems and services. MNIT will proactively identify and communicate to the Agency any system risks, vulnerabilities, weaknesses, threats or gaps that put the Agency at risk and identify options for change to address the risk, within the parameters and limits of the resources available to MNIT. MNIT is not responsible for maintaining internal controls for Agency non-IT related business.
- MNIT will collaborate with the Agency to comply with all applicable state and federal laws, rules and regulations that affect all consolidated agencies, boards, and councils. MNIT will work with the Agency to comply with the additional agency-specific legal and/or regulatory, safety and security requirements, and state standards. If the Agency is not currently in compliance, additional resources may be required to bring the Agency into compliance.
- Provide timely, accurate invoices to the Agency at a level of detail necessary for the Agency to identify the appropriate funding source from which to make payment, and respond to agency billing questions.

- Provide regular volume, rate, and cost information to the Agency timely and sufficient for the Agency to plan, manage, and commit funding for Agency IT services, fiscal operations, and functions related to the CBTO and other MNIT employees. Collaborate with Agency to provide information timely for decision making.
- Develop and maintain IT disaster recovery plans and procedures for the recovery of the state's executive branch technology systems in case of system or IT service interruption or failure. MNIT will collaborate with executive branch state agencies' continuity of operations designated staff to develop and maintain recovery strategies consistent with business priorities, timelines, and resources. MNIT will coordinate and communicate response and recovery activities and timelines with executive branch state agencies' continuity of operations designated staff during a system or IT service interruption or failure. MNIT will also collaborate with executive branch state agencies' continuity of operations designated staff on training, testing, and exercise activities to determine and improve the effectiveness of IT disaster recovery plans and procedures consistent with business priorities, timelines, and resources. IT disaster recovery planning, training, and exercises will be conducted in accordance with federal and state standards and guidelines, including the MNIT Information Technology Disaster Recovery Planning Standard.

## The Agency Roles and Responsibilities

---

The Agency has the responsibility to:

- Ensure the CBTO is in a role within the Agency that directly communicates with the Commissioner, Deputy Commissioner(s), or equivalent.
- Include the CBTO as a regular attendee of Agency leadership team meetings to provide IT-related reports and work in partnership with the Agency to enable MNIT IT strategy to support the business needs of the Agency.
- Provide feedback to MNIT's Commissioner regarding the performance of the Agency's CBTO as the Agency deems appropriate.
- Work with MNIT to perform a portion of the other administrative services and partner with MNIT on legislative functions, as needed and agreed upon by the parties to this SLA. (Specific services will be added to the local services section of this document.)
- Collaborate with MNIT to identify and enable Agency compliance with all applicable state and federal laws, rules, standards and regulations relating to the agency's IT services. If the Agency is not currently in compliance, additional resources may be required to bring the Agency into compliance.
- Process and pay all invoices to MNIT in a timely manner. The Agency may request a credit or an amendment to a bill if there is an error.

- Work collaboratively with MNIT and the CBTO to adhere to the policies, processes and procedures for requesting and maintaining IT services and tools, and participate in IT project management methodologies.
- Collaborate with MNIT on MNIT's Asset Management and Inventory to provide proper accounting for IT assets at the Agency, in compliance with federal and state statutory and regulatory requirements and policies.
- Determine and communicate new service requirements to the CBTO based on Agency needs including, but not limited to, changes in service volumes and IT projects, identifying funds for new services and investments, and initiating a change to this SLA and/or the IT Budget, as prescribed by the SLA and this Section.
- Unless otherwise approved by MNIT's Commissioner, provide at least 30 calendar days' notice to MNIT of cancellation of projects and termination of services. This is required because MNIT is obligated under labor agreements to provide staff with a 21-day notice of layoffs.
- Work with its CBTO to provide necessary financial accounting services and purchasing of IT goods and services for the Agency. Provide regular and timely financial reporting sufficient to plan, manage and commit funding for Agency IT services, fiscal operations and functions related to the CBTO and other MNIT employees.
- Develop and maintain a continuity of operations plan and procedures that include the Agency's business priorities, timelines and critical information needs. Collaborate with MNIT to develop recovery strategies for the critical telecommunications and technology systems and services needed to support business services. Coordinate and communicate response and recovery activities with MNIT during a continuity incident, emergency or disaster. Work jointly with MNIT on training, testing and exercise activities to determine and improve the effectiveness of continuity plans and procedures.
- Provide oversight, leadership, and direction for Agency IT investments and services.

## **The Chief Business Technology Officer Roles and Responsibilities**

---

The CBTO represents MNIT at the Agency, oversees all Agency-based MNIT resources and employees, and reports to MNIT. The CBTO is responsible for maintaining a strong and collaborative partnership with the Agency. The CBTO has the authority and responsibility to:

- Hire and manage MNIT employees in coordination with MNIT Human Resources.
- Represent MNIT in communications with Agency leadership regarding the Agency's needs for IT services to support the Agency's unique business operations and priorities.

- Ensure that the Agency is made aware of and implements all applicable MNIT IT policies, standards, guidelines, direction, strategies, procedures and decisions. Where the Agency does not implement the aforementioned, the CBTO will inform the Agency where and how the Agency is assuming risk. The CBTO will work with the Agency to identify and avoid risks that the Agency cannot assume because they would impair other agencies, boards, or councils.
- Report directly to, and be held accountable by MNIT for IT operational direction including, but not limited to, IT-related planning activities, purchasing, security, policy implementation and management of MNIT employees.
- Maintain regular dialog with the Agency's senior leadership to ensure that the SLA performance expectations reflect the current Agency needs and that the Agency is receiving the services it needs.
- Manage within the Agency-approved IT Budget, including determining service delivery strategies in consultation with the Agency. Work with Agency to enable shared understanding of MNIT financial accounting and IT management and purchasing for the Agency. Provide regular financial reporting sufficient for the Agency to plan, manage, and commit funding for IT services and other IT operations.

## Data Handling Roles and Responsibilities

---

- The Agency's electronic data that is housed on MNIT-managed technology belongs to the Agency and is subject to the Agency's direction and control. The State Chief Information Officer is not the responsible authority under Minnesota Statutes, Chapter 13 (the Data Practices Act) for the Agency's data that resides on MNIT managed technology equipment. Agencies will work collaboratively with MNIT to ensure that MNIT has the appropriate resources to adhere to all policies and requirements provided by the Agency in order to protect the Agency's data.
- Should MNIT receive a data request for the Agency's data, MNIT will not produce the requested data. However, MNIT will notify the Agency and will assist in retrieving the data housed on MNIT-managed technology, if requested by the Agency to do so.
- Should an Agency receive a request for MNIT data, the Agency will not produce the requested data. The Agency will notify MNIT that it received the request.
- Should a request include Agency data and MNIT data, MNIT and the Agency will work together to appropriately respond to the request.
- Minnesota Statutes, Chapter 16E, requires the Agency to share data, including not public Agency data, with MNIT as necessary for MNIT to provide IT services and equipment to the Agency. Sharing data as required by Chapter 16E, and in the manner prescribed in the Data Practices Act, does not affect the classification of any not public

data shared with MNIT and is not intended to and does not waive any privileges afforded to not public data under applicable law. MNIT and the Agency must continue to protect any not public data as required by law.

- In accordance with the Data Practices Act, MNIT will only access and use not public Agency data to the extent necessary for a work assignment or project on behalf of the Agency.
- Should MNIT or the Agency become aware of a known or suspected security incident or potential breach of an Agency's electronic data, each will promptly notify the other. MNIT will work to identify the deficiency that led to the breach and to correct, mitigate and remediate the deficiency, which may require additional Agency resources. The Agency and MNIT will coordinate a response and work cooperatively to resolve the incident and comply with the notice and regulatory requirements under applicable state and federal law.
- This SLA is not meant to supersede, waive, or violate data handling roles and responsibilities set forth in state law, federal law, or any applicable data sharing and/or business associate agreement between MNIT and Agency.

## Budget Scope

---

Enterprise rate-based services and services provided by the CBTO will be billed directly to the Agency. The CBTO will work with the Agency's designated senior leadership staff person, Chief Financial Officer (CFO), and other appropriate finance staff as designated by the CFO to develop a budget for local services, and to ensure that all IT expenditures for the Agency are accounted for, such as staffing, hardware, software, supplies, training, and administrative costs. All IT budget expenditures must be approved by the CBTO or delegate.

MNIT and the Agency will collaborate to determine appropriate accounting processes to support the Agency's payment of all MNIT bills. MNIT and the Agency will cooperatively plan and communicate regarding IT expenditures and billing.

## Acceptance

---

In the IT Consolidation Act, the Minnesota Legislature required the Chief Information Officer to enter into a Service Level Agreement governing the provision of IT systems and services, assets, and personnel with each state agency. STATE GOVERNMENT, INNOVATIONS AND VETERANS OMNIBUS BILL, 2011 Minn. Session Law Serv. 1st Special Session, Ch. 10, Art. 4 (S.F. 12).

For the departments, agencies, offices, councils, boards, commissions and other entities in the executive branch of Minnesota State government that are subject to IT Consolidation, the use of MNIT is required by the State Legislature. MNIT recognizes that providing IT services is most successfully done in close



partnership with the Agency. MNIT and the Agency representative will memorialize their formal partnership by adding their signatures to this document.

## **Dispute Management**

---

The parties agree to cooperate with each other in the performance of the duties and responsibilities under this SLA. Each party to this SLA will make every effort to avoid disputes by clearly documenting communication and engaging the applicable chain of command as necessary. If the parties are unable to reach an agreement with respect to any dispute related to the services, terms, and provisions of this SLA, the Agency's Commissioner/CEO/Executive Director and MNIT's Commissioner will meet to determine further action. If no agreement can be reached, the Agency and MNIT will participate in conflict resolution proceedings managed by the Bureau of Mediation Services.

## **Liability**

---

Each party shall be responsible for claims, losses, damages and expenses which are proximately caused by the acts or omissions, including lack of funding, of that party or its agents, employees or representatives acting within the scope of their duties, subject to the limitations provided by law, and will not be responsible for the acts or omissions of the other party or its agents, employees or representatives, or the results thereof. Minn. Stat. § 3.736 shall govern the liability of each party. Nothing herein shall be construed to limit either party from asserting against third parties any defenses or immunities (including common law, statutory and constitutional) it may have, nor shall anything herein be construed to create a basis for any claim or suit when none would otherwise exist. This provision shall survive the termination of this SLA.

## **Additional Provisions**

---

The terms of this SLA are not intended to supersede or violate any applicable bargaining unit contracts, state laws, or federal laws. If any provision of this SLA is determined to be unenforceable, then such provision will be modified to reflect the parties' intention. All remaining provisions of this SLA shall remain in full force and effect.

## **Law to Govern**

---

This SLA shall be interpreted and enforced in accordance with the laws of the State of Minnesota. Any legal proceedings arising out of this SLA, or breach thereof, shall be adjudicated in the state courts of Minnesota, and venued in Ramsey County, Minnesota.

## Assignment

---

Neither MNIT nor the Agency shall assign or transfer any rights or obligations under this SLA without the prior written consent of the other party. This provision must not be construed to limit MNIT's or the Agency's ability to use third party contractors or products to meet its obligations under this SLA.

## Section 2: Service Agreement – Projects and Services

*Version FY22-23*

This section provides information related to the various projects and services provided to agencies. Further information on each project or service is available through the agency based CBTO or their designee.

### Projects

---

Definitions:

- **Project:** a temporary endeavor undertaken to create a unique product, service or result. It has a start date, specific goals and conditions, defined responsibilities, a budget, a plan, and end date. Examples include, but are not limited to, developing a new product or service, developing or acquiring a new or modified information system, upgrades, and releases.
- **IT Project:** an effort to acquire or produce information and telecommunications technology systems and services.
- **Total expected project cost:** direct staff costs, all supplemental contract staff and vendor costs, and costs of hardware and software development or purchase.

Projects can have multiple funding sources including:

- A specific legislative appropriation called a Biennial IT (BIT) project.
- A 2001 fund allocation known as an Odyssey Fund project.
- An internal agency budget allocation known as an Agency Funded project.

Each of these project types is documented in the MNIT Enterprise Engagement Program Management Office (EPPMO) project and program management system. Projects documented in this fashion are incorporated by reference in this SLA. Documentation on each project is available through the agency based CBTO or their designee.

## Services

---

There are five types of services available:

1. **Enterprise Services\*** are standard services that all executive branch agencies are required to utilize to ensure consistency and business interoperability within government. Examples include: email and calendaring, phones, networks, servers, desktop/laptop computers and related support services. These services have biennial enterprise rates approved by Minnesota Management and Budget (MMB) and are uniform across all agencies. *For more specific service information, please refer to the Enterprise Services descriptions in Section 2.*
2. **Shared Services\*** are standard services that executive branch agencies may utilize to support their business operations. Alternatively, this type of service may also be provided on a single agency basis by MNIT staff partnering with agencies. An example is Geospatial services. This service has biennial enterprise rates approved by MMB and are uniform across all agencies that utilize the shared service. *For specific service information, please refer to the Shared Services description in Section 2*
3. **Center of Excellence Services** are services that executive branch agencies may utilize to support their business operations. Typically, these services are provided to multiple agencies by MNIT staff located at a single agency office. An example is Salesforce Development and Support (SFDC) – Center of Excellence (COE), provided by MNIT@DEED staff and used by several other agencies. These services have rates set by the service provider and approved by MMB and are uniform across all agencies that utilize the service. *For specific service information, please refer to the Center of Excellence Services description in Section 2*
4. **Local Services** are services that are provided by MNIT staff located at an agency office and are provided to serve business operations specifically for that agency. Examples include: Application Support and Development, Application Management, Application Operations, Project Management Office functions including Project Management, Business Analyst and Quality Assurance functions. These services are provided on a ‘pass-through’ basis for staff salaries and benefits, and any IT purchases not covered by an Enterprise, Shared, or Center of Excellence Services. *For specific service information, please refer to the Local Services description in Section 2*
5. **Enterprise Security Services\*** are provided to all MNIT executive branch customers at a core level. These services include: Security Operations, Threat and Vulnerability Management, Access and Identity Management, and Governance, Risk, and Compliance. Within these services, additional protective services are provided. *For specific service information, please refer to the Enterprise Security Services description in Section 2*

\*A detailed description of each service, pricing and delivery terms associated with that service may be found on the [MNIT public website](#).

Services documented in this fashion are incorporated by reference in this SLA.

### **Center of Excellence Services Summary**

<b>Service Details</b>	<b>Summary Description</b>
Supporting Agency	Department of Employment and Economic Development
Service Name	Salesforce Development and Support (SFDC) – Center of Excellence
Included	<ul style="list-style-type: none"> <li>Development services, licensing, storage, platform support, add-on software, professional services.</li> </ul>
NOT included	<ul style="list-style-type: none"> <li>Direct end user support of delivered solutions. Customers must respond to end users and escalate support requests to the MNIT when necessary.</li> </ul>
Delivery Method	<ul style="list-style-type: none"> <li>Service agreements define project scope, deliverables, and development resources. Professional services hours are billed for development and support.</li> </ul>
Hours of Operation	<ul style="list-style-type: none"> <li>Production availability 7x24x365</li> </ul>

**Local Services Summary** *For detail, please refer to Local Services description(s) in Section 2*

**Enterprise Security Services Summary** *For detail, please refer to the Enterprise Security Services description in Section 2*

# Service Name: Database Support - Shared Services

Revision Date 10/28/2021

## Executive Summary

Service Details	Summary Description
Service Name	<a href="#">Database Administration</a>
Included	<ul style="list-style-type: none"> <li>Database operational support</li> </ul>
NOT included	<ul style="list-style-type: none"> <li>Database logical design</li> <li>Application support</li> <li>Dedicated host, license &amp; maintenance costs</li> </ul>
Delivery Method	<ul style="list-style-type: none"> <li>Fulltime support staff with access to MNIT on-premises and external cloud environments</li> </ul>
Hours of Operation	<ul style="list-style-type: none"> <li>Production availability 7x24</li> <li>On-call off hours, weekends, and holidays</li> <li>Non-production: M-F; 7 a.m.-5 p.m.</li> </ul>

## Description

Database Support Services offered by Minnesota IT Services (MNIT) manage highly available and secure environments for agency databases.

Database services includes support for Oracle, Microsoft SQL Server, and IBM DB2 databases. DB2 is supported on the IBM Mainframe (DB2 zOS) and on distributed platforms (DB2 LUW). All three types of databases may be hosted on dedicated servers/Virtual Machines (VM) or on multi-tenant hosts provided by MNIT Database Shared Services for Oracle and Microsoft SQL Server.

- Dedicated Server/VM Databases:
  - Databases on distributed platforms that are large, complex, have high volume workloads or compliance requirements which mandate database segregation are hosted on dedicated servers/VMs. Customers may choose to have dedicated hosts for databases based solely on a preference for a segregated database environment for their application.

- Multi-Tenant Shared Database Services:
  - MNIT Shared Database Hosting provides a lower cost option for customer applications in a multi-tenant environment. Databases in the shared hosting environment should fit all these criteria: small, simple, and low volume workloads.

**MNIT Shared Services Database Administrators** (DBA) staff are responsible for the build and all operational aspects of the database environment and for the physical administration of the database.

**MNIT @agency application staff and data base administrators** (DBAs) are responsible for the logical design and definition of the database – the data definition library (DDL) and all data content.

**\*\*These roles free MNIT staff at partner agencies to focus on the application and business issues.**

## What systems or services are supported?

---

### Distributed systems supported database management software

- Oracle
- Microsoft SQL Server
- IBM DB2

### Mainframe supported database management software

- IBM DB2

## What services are included?

---

### All Database Services include:

- Installation, administration, backup configuration and recovery processes, performance tuning, product life cycle management, environment management, monitoring, and database capacity management.
- 24x7 technical support is available for production databases.

### Shared Database Hosting also includes:

- Database license and software costs
- Mainframe/Server/VM charges (except database storage)
- Annual database software maintenance

## What services are NOT included?

---

Management and use of the business side application

### Shared SQL Database Hosting does not include:

- Database storage costs

### Dedicated Hosted Database Support does not include:

- Database license and software purchase costs
- Dedicated Server/VM monthly charges
  - *See Hosting Service Description for more information*
- Annual software maintenance

## How will the service be delivered?

---

- Fulltime support staff
- Either from the MNIT on-premises or external cloud computing environments, depending on business needs or requirements

## What are the hours of operation and how to get support?

---

- Service hours for Production:
  - 24x7x365
  - Prime support hours: M-F; 7 a.m.-5 p.m. (except holidays)
  - On-call during off hours and all-day Saturdays, Sundays, and holidays
- Service hours for Non-Production
  - Prime support hours: M-F; 7 a.m.-5 p.m.
- Submit requests through the online Minnesota Service Hub
- Submit break/fix incidents through the MNIT Service Desk



## What will the response time be?

Response Level	Definition	Example	Response Target	Return to Service Target
Priority 1 Critical	<p>The hosted website is not operational for multiple users, or citizens during scheduled availability</p> <p>A major function of the hosting service is not operational for multiple users during the hours that the service is scheduled for availability</p>	A production site displays that an application is unavailable	15 minutes	2 hours
Priority 2 High	<p>A user needs administrative assistance performing urgent updates or maintenance</p> <p>A minor function of the hosting service is not operational for many users (who can continue to use other application functions)</p>	Application support staff are reporting issues of concern related to aspects of production processing	2 hours	12 hours
Priority 3 Med	<p>A minor function of the hosting service is not operational for one or few users (who can continue to use other application functions)</p> <p>A user has questions about the hosting service functionality or needs assistance in using the service</p>	Application support staff are reporting issues of limited concern related to one aspect of processing	8 hours	72 hours
Priority 4 Low	The hosting service is not operational for one or few users outside of the hours of availability – and is not impacting citizen facing services or sites	One person reports an issue with a database user account.	2 business days	120 hours

\*\*Percentage meeting Return to Service Target by Year and Month: 80%\*\*

## What are the business responsibilities?

---

All installations are subject to a design process between MNIT and the subscriber. This process will ensure the subscriber's needs are met while adhering to MNIT Managed Hosting design requirements.

The customer is responsible for the following:

- Submit requests through the online Minnesota Service Hub:
  - Requests for new databases
    - Provide a detailed application requirements list
    - Provide detailed design document(s) approved by MNIT Cloud Architecture and Secure Engineering
    - Provide Data Definition Language (DDL) to describe the data and information structures
  - Requests for modifying database structures
  - Requests for data refreshes
  - Requests for decommissioning of old databases
- Submit break/fix incidents through the MNIT Service Desk
- Provide Extract, Transform and Load (ETL) scripts to perform data loads into information structures
- Provide resources to perform systems testing as needed
- Provide customer contact information, customer number and charge number

## When will regular maintenance be performed?

---

- As updates and patches are provided from the software vendor
- Any updates are planned, scheduled, and performed within the existing change management windows

## Change Management Process/Termination

---

MNIT follows established enterprise change management procedures and processes.

# Service Name: Enterprise Hosting

Revision Date 10/18/2021

## Executive Summary

Service Details	Summary Description
Service Name	Enterprise Hosting Services
Included	<ul style="list-style-type: none"> <li>• Data Center Services and Support</li> <li>• Enterprise Cloud Services</li> <li>• Virtual Desktop</li> <li>• Enterprise Secure File Transfer Protocol (SFTP)</li> <li>• Physical and virtual server management and support</li> </ul>
NOT included	<ul style="list-style-type: none"> <li>• Customer application support</li> </ul>
Delivery Method	<ul style="list-style-type: none"> <li>• Fulltime support staff</li> <li>• Server equipment and infrastructure both on premise and in the cloud</li> </ul>
Hours of Operation	<ul style="list-style-type: none"> <li>• 24x7x365 expected infrastructure up time</li> <li>• On premise support:               <ul style="list-style-type: none"> <li>○ Monday through Friday, 6 a.m.-6 p.m.</li> </ul> </li> <li>• On call support:               <ul style="list-style-type: none"> <li>○ Monday–Friday 6p.m. to 6 a.m.</li> <li>○ Saturday, Sunday and Holidays</li> </ul> </li> </ul>

## Description

Enterprise Hosting Services consist of many components that comprise a highly available and secure environment to house agency applications and systems.

The specific quantity and location of any component will be decided by the requirements of each application and system. Ongoing management and analysis will ensure that system components are configured and maintained to meet agency partner needs.

Periodic reviews are conducted of the prescribed services currently in use. Agency partners will be given opportunity to refine the current environment to ensure the agency environment is running efficiently and that resources are not over- or under-allocated or provisioned. Adjustments can ensure the

resources align properly with the business requirements. Pre-determined standards for consistent management and support are utilized. The following features apply to all hosting services:

- All Shared Hosting environments are built and configured with hardware redundancy within the Data Centers, but not between the Data Centers to ensure the Compute Infrastructure stays up and running.
- All environments are updated and managed to ensure that any changes or updates to the application are met.
- The hosting environment will allow for continued evaluation and modification to the existing environment, to meet technical or budgetary requirements.
- All services are designed and built according to Minnesota IT Services security standards, policies and governance requirements.

## What systems or services are supported?

---

- Compute
- Storage
- Data center network
- Space and utilities
- Security
- Software licensing
- Management tools

## What services are included?

---

- Hosting – Data Center RU (Rack Units / Physical Hosting)
- Hosting – Dedicated Server
- Hosting – Shared Hosting (Virtualization vCPU & vRAM)
- Hosting – Data Storage
- Hosting – Cloud Hosting (Compute and Data Storage)
- Hosting – Enterprise SFTP
- Hosting – Enterprise Virtual Desktop
- Data Storage Backups
- Data center network connectivity
- Space and utilities
- Security
- Software licensing
- Management tools

## **What services are NOT included?**

---

- WAN connectivity
- Mainframe services
- Management and use of the business side application
- Application and database licensing
- Disaster Recovery

## **How will the service be delivered?**

---

- Full time MNIT support staff
- Provided server equipment and infrastructure
- Either on Premise or in the Cloud depending on needs or requirements

## **What are the hours of operation and how to get support?**

---

- 24x7x365 expected infrastructure up time.
- M-F, 6 a.m.-6 p.m. on premise support staff; On-call off hours and all-day Saturday and Sunday.
- Submit routine requests to the MNIT Service Hub
- Submit break/fix incidents through MNIT Service Desk

## What will the response time be?

---

Response Level	Definition	Example	Response Target	Return to Service Target
Priority 1 Critical	<p>The hosted website is not operational for multiple users, or citizens during scheduled availability.</p> <p>A major function of the hosting service is not operational for multiple users during the hours that the service is scheduled for availability.</p>	Site displays a 404 page not found error.	15 minutes	2 hours
Priority 2 High	<p>A user has questions about functionality or needs assistance in using the service.</p> <p>A user needs administrative assistance performing urgent updates or maintenance.</p> <p>A minor function of the hosting service is not operational for many users (who can continue to use other application functions).</p>	Web Administrators are unable to access FTP or ROOT folders to update security related issues, contents, and site functionality.	2 hours	8 hours
Priority 3 Med	A minor function of the hosting service is not operational for one or few users (who can continue to use other application functions).	Web Administrators are unable to access FTP or ROOT folders to update low priority contents/verbiage.	8 hours	2 business days
Priority 4 Low	The hosting service is not operational for one or few users outside the hours of availability – and is not impacting citizen facing services or sites.	One person reports issue with their browser displaying page content.	2 business days	5 business days

## What are the business responsibilities?

---

- Assist in creating realistic expectations.
- Submit requests for new hosting environment.

- Submit request to change existing hosting environment.
- Submit request to decommission existing hosting environment.
- Report any issues as soon as possible through the Minnesota IT Service Hub or by contacting the MNIT Enterprise Service Desk.

## When will regular maintenance be performed?

---

- As updates and patches are provided from the equipment manufacturer or software provider.
- Any updates are planned, scheduled and performed within the existing change management windows.

## Change Management Process/Termination

---

Minnesota IT Services follows established enterprise change management procedures and processes.

# Service Name: Local Area Network (LAN) Services

Revision Date 09/01/2021

## Executive Summary

---

Service Details	Summary Description
Service Name	<a href="#">LAN</a>
Included	<ul style="list-style-type: none"> <li>• Wired and wireless IP network connections within a location or campus</li> </ul>
NOT included	<ul style="list-style-type: none"> <li>• Wide area network (WAN) connections</li> </ul>
Delivery Method	<ul style="list-style-type: none"> <li>• Minnesota IT Services owned and managed LAN devices</li> </ul>
Hours of Operation	<ul style="list-style-type: none"> <li>• 24x7x365</li> </ul>

## Description

---

LAN services from Minnesota IT Services provide secure network connections to a user's computing device. These connections enable access to network-based information, resources and services that employees need to do work. LAN services generally operate within a building or campus and provide connections to the state network known as Minnesota's Network for Enterprise Technology (MNET). Network connections may be wired or wireless. LAN ports also support the Ethernet connection of wired devices besides computers such as printers, file/print servers, IP telephones, videoconferencing codecs, wireless access points, and security monitoring devices.

## What systems or services are supported?

---

- Install and configure LAN premise equipment and connect to structured cabling systems
- LAN devices: Up/down, standard operation and correct configuration
- LAN firewall service: Up/down, standard operation and correct configuration
- Provide, monitor and manage LAN equipment with enterprise tools and inventory systems
- Manage a distributed LAN equipment spares inventory
- Manage structured cabling and associated infrastructure
- Arrange for on-site technical support as needed

## What services are included?

---

LAN services provides infrastructure within a building or campus environment, which enables IP-based data, voice and video communications among local resources within an organization. LAN services support the infrastructure components (wired and wireless) and resources required to enable connectivity from end user computing devices. The service includes equipment, maintenance, configuration, administration, monitoring, and support of the agency premise networking infrastructure.

## What services are NOT included?

---

- Fiber-based installation: For large construction, remodeling and office moves, LAN architecture and detailed design work is billed per installation.
- LAN structured cabling systems: One-time charges for installation, update or repair of LAN wiring systems (cabling, wall plates, patch panels, etc.) are billed per installation.

## How will the service be delivered?

---

Each MNIT Enterprise Services customer has a designated Enterprise Services Relationship Manager who works with the customer on an individual basis for their IT service needs. In partnership with the Installation Coordinators and Service Managers, the Relationship Manager:



- Facilitates service implementation.
- Coordinates Minnesota IT Services staff and resources as needed.
- Provides consultation, needs assessment, analysis, and cost-effective solutions.
- Develops proposals and service agreements.
- Assists with writing procurement specifications.

## What are the hours of operation and how to get support?

---

### Minnesota IT Services Service Desk Contacts

- **Business Hours:** 24 x 7
- **Contact Name:** Minnesota IT Services Service Desk
- **Phone Number:** 651-297-1111
- **Website and Service Catalog:** [mn.gov/Minnesota IT Services](http://mn.gov/Minnesota%20IT%20Services)

## What will the response time be?

Response Level	Definition	Example	Response Target	Return to Service Target
Priority 1 Critical	Any Incident that has “massive impact” and is highly visible, impacts a significant number of Users, a major agency, application or service, and has no redundancy or alternate path.	A LAN CORE and associated access switch infrastructure is in a degraded state or non-functional for all users at a large office site or a designated mission critical site.	15 minutes	2 hours* * Business Hours
Priority 2 High	Incident deemed to have a high impact by being highly visible, impacting a significant number of users, impacting a major agency, application or service, where there is no redundancy or alternate path, and a bypass is unavailable.	A LAN switch is non-functional for a group of users connected to that LAN device.	2 hours	8 hours* * Business Hours
Priority 3 Med	Incident deemed to have a medium impact by being visible, impacting a limited number of users, where a resource or service is down or degraded.	A LAN connection to an individual user is not working or the LAN switch uplink path is at bandwidth capacity, or a WLAN AP has limited capacity.	8 hours	2 business days
Priority 4 Low	Any incident that impacts a small number of users or a single user where a resource or non-critical service is down or degraded and a deferred fix or maintenance is acceptable.	LAN individual home user has intermittent connection issues	4 hours	5 business days

## What are the business responsibilities?

- Designate a 24 x 7 point of contact for each building or campus LAN environment, and provide access to buildings, communications rooms and other facilities as needed.
- Provide electrical power to LAN infrastructure devices.

- Ensure that each location meets Minnesota IT Services minimum standards including documentation, wiring, power, HVAC, access, and security. Please contact the Minnesota IT Services Service Desk for a detailed list of requirements.
- The cost of the design, planning, installation, replacement or repair of structured cabling/wiring used for LAN services.
- Ensure that all local area network users obtain network access only with their own user IDs.
- When calling in a problem, provide as much relevant information as possible to help troubleshooting and resolution.

## **When will regular maintenance be performed?**

---

To ensure optimal performance of LAN services, routine maintenance will be performed on a regular basis by MNIT Services staff and their external partners. The service unavailability during scheduled maintenance windows will be excluded from the uptime calculations.

MNIT Services will provide customers a 5-business day advance notice of scheduled maintenance. All prescheduled systems maintenance, unless otherwise agreed upon in advance, shall be performed on the following schedule:

- Monday - Friday: 2 a.m. to 6 a.m. CDT
- Saturday: 2 a.m. to noon CDT

## **Change Management Process/Termination**

---

MNIT follows established enterprise change management procedures and processes.

# Service Name: Middleware Support - Shared Services

Revision Date 09/15/2021

## Executive Summary

Service Details	Summary Description
Service Name	<a href="#">Middleware</a>
Included	<ul style="list-style-type: none"> <li>Middleware software and support</li> </ul>
NOT included	<ul style="list-style-type: none"> <li>Customer application support</li> <li>Database charges if MQ messaging is employed</li> <li>Dedicated host charges</li> </ul>
Delivery Method	<ul style="list-style-type: none"> <li>Fulltime support staff with access to the MNIT on premise and external cloud environments</li> </ul>
Hours of Operation	<ul style="list-style-type: none"> <li>Production: availability 7x24x365</li> <li>On-call off hours, weekends, and holidays</li> <li>Non-production: M-F; 7 a.m.-5 p.m.</li> </ul>

## Description

Middleware software manages communication between an application's component parts (web, application, and database hosts/VMs) by providing services that enable concurrency, transaction management and messaging. Middleware software sits between the operating system and the application code. Middleware simplifies the leveraging of services within the application environment, as well as with other applications.

- Tier 1 consists of a Middleware instance on an application server/VM and use of shared platforms for web presentation services
- Tier 2 is an add-on option to Tier 1 for using dedicated host/VM(s) for web presentation or other services, instead of using shared multi-tenant hosts.

## What systems or services are supported?

### Distributed systems supported software

- WebSphere
- JBoss

- Tomcat
- MQSeries

### **Mainframe supported software**

- CICS
- MQSeries

## **What services are included?**

---

### **All Middleware Support Services include:**

- All Middleware support services include software installation, implementation, design assistance and administration, as well as ongoing support for deployments, administration tools, monitoring, maintenance and patching, service coordination, role-based access security, upgrades, backup configuration and recovery procedures.
- 24x7x365 technical support is available for production instances.

### **Middleware Tier-1 also includes:**

- Middleware software license
- Annual software maintenance

## **What services are NOT included?**

---

- Management and use of the business side application
- Database charges for advanced message queue systems (MQS) databases used by Middleware for asynchronous messaging between applications

*See Database Service Description for more information*

### **Middleware Tier-1 does not include:**

- Dedicated application server/VM charges

*See Hosting Service Description for more information*

### **Middleware Tier-2 does not include:**

- Dedicated Web presentation or other services - server/VM charges

*See Hosting Service Description for more information*

## How will the service be delivered?

---

- Fulltime support staff
- Either from the MNIT on-premises or external cloud computing environments, depending on business needs or requirements

## What are the hours of operation and how to get support?

---

- Service hours for Production
  - 7x24x365
  - Prime support hours: M-F; 7 a.m.-5 p.m. (except holidays)
  - On-call during off hours and all-day Saturdays, Sundays, and holidays
- Service hours for Non-Production
  - Prime support hours: M-F; 7 a.m.-5 p.m.
- Submit requests through the online Minnesota Service Hub
- Submit break/fix incidents through the MNIT Service Desk

## What is the response time?

---

Response Level	Issue Definition	Example	Response Target	Return to Service Target
Priority 1 Critical	<p>The middleware-hosted application is not operational for multiple users during scheduled availability.</p> <p>A major function of a middleware-hosted application is not operational for multiple users during the hours that the service is scheduled for availability.</p>	<p>A production application site is unresponsive to a request.</p> <p>A security exposure has been identified and needs urgent resolution.</p>	15 minutes	2 hours
Priority 2 High	<p>A customer needs to have urgent updates or urgent maintenance applied to Middleware infrastructure.</p> <p>A minor function of a Middleware-hosted application is not operational for many users (who can continue to use other application functions).</p>	<p>A production application site functionality is returning unusual results.</p>	2 hours	12 hours
Priority 3 Med	<p>A minor function of a middleware-hosted application is not operational for one or few users (who can access other application functions).</p> <p>A user has questions about the middleware service functionality, needs assistance in using the service or is requesting Middleware configuration changes.</p>	<p>Application site functionality is returning unusual results.</p> <p>A help desk work request is received asking for middleware configuration changes.</p>	8 hours	72 hours
Priority 4 Low	<p>The middleware application hosting service is not operational for one or few users outside of the hours of availability – and is not impacting citizen facing services or sites.</p> <p>A customer has questions requiring research about the middleware service functionality or needs assistance in researching the technology used in the middleware service.</p>	<p>One person reports an issue with the browser displaying application page content.</p> <p>A customer submits a request to the help desk requiring middleware product research.</p>	2 business days	120 hours

---

## What are the business responsibilities?

---

All installations are subject to a design process between MNIT and the subscriber. This process will ensure the subscriber's needs are met while adhering to MNIT Managed Hosting design requirements.

The customer is responsible for the following:

- Submit requests through the online Minnesota Service Hub:
  - Requests for new Middleware implementations
    - Provide a detailed application requirements list
  - Requests for modifying Middleware configurations
  - Other service requests and inquiries
  - Decommissioning requests for Middleware instances
- Submit break/fix incidents through the MNIT Service Desk
- Work with Enterprise Monitoring group if synthetic transaction monitoring is required
- Provide resources to perform systems testing as needed
- Provide customer contact information, customer number and charge number

## When will regular maintenance be performed?

---

- As updates and patches are provided from the software vendor.
- Any updates are planned, scheduled, and performed within the existing change management windows.

## Change Management Process/Termination

---

MNIT follows established enterprise change management procedures and processes.



# Service Name: Minnesota Enterprise Identity and Access Management (MNEIAM)

Revision Date 02/10/2022

## Executive Summary

---

Service Details	Summary Description
Service Name	MN Enterprise Identity and Access Management (MNEIAM) – Enterprise Service
Included	Oracle IAM on-prem suite and Oracle IDCS SaaS, IAM Database in Exadata appliance, and Middleware technology
NOT included	Load balancer, and firewall
Delivery Method	Service can be requested via the Minnesota Service Hub and supported by full time support staff.
Hours of Operation	24 x7 with multi-datacenter architecture to provide high availability / up-time service of IAM system.

## Description

---

The Minnesota Enterprise Identity Access Management (MNEIAM) Service provides user authentication and management services when accessing data via webpages. It is commonly used to allow public service employees, the general public and service providers, to connect with restricted state websites.

## What systems or services are supported?

---

MNEIAM, which comprises Oracle IAM software suites 11g Patch Set 3 (OIM, OAM/OIF, OUD, OVD, and OHS) and Oracle IDCS SaaS is configured to provide High Availability (HA) / Uptime and to support multiple agency integration. The MNEIAM Database runs on Oracle Exadata appliances between two datacenters. In addition, the MNEIAM system utilizes the middleware technology that runs on virtual service instances to fully support the system.

## What services are included?

---

- Work with MN state agency business and technical staff to coordinate the hand-off into and out of the service.
- On-board new applications for agencies.
- Maintain the MNEIAM software and database environment, including evaluating and implementing updates and patches as appropriate.
- Provide authentication and authorization screens for end-users.
- Provide MNEIAM-specific support to other services. End users would continue to work directly with existing call centers.
- MNIT offers a Basic and an Advanced MNEIAM package of features and benefits.

## What services are NOT included?

---

- Load balancer, and firewall.
- Website creation, and specific website data beyond authentication.

## How will the service be delivered?

---

- The MNEIAM service can be requested via the Minnesota Service Hub
- Support by full time MNIT Enterprise staff
- Change and release management will be engaged to deliver the services that are requested through the service management tool.

## What are the hours of operation and how to get support?

---

- During regular business hours of 6am to 6pm Central Time, the MNEIAM system will be supported with state IAM support staffs, and by an on-call IAM staff during off-hours. Currently, we have a contracting team who is also supporting the system at the time of an escalated support request.

---

## What will the response time be?

---

<i><b>Incident Level</b></i>	<i><b>Definition</b></i>
Critical (Severity 1)	Potential for significant impact on client operations; multiple applications impacted, and large number of customers impacted; risk to the overall environment is large
High (Severity 2)	High incident can be described as an event affecting a lesser percentage of application or users; critical functionality or accessibility interrupted, degraded or unusable, having a severe impact on service availability. No acceptable work around or alternative.
Medium (Severity 3)	Minimal impact to operations; one or two applications impacted; intermittent availability issue with no work around available; poses minor risk to the environment
Low / Best Effort (Severity 4)	Little impact on client operations; one or two individuals impacted; intermittent issues, does not pose a risk to the environment

The table below shows production response times.

<b>Response Level</b>	<b>Definition</b>	<b>Example</b>	<b>Response Target</b>	<b>Return to Service Target</b>
Severity 1 (P1)	Critical	Yes (call required and tech bridge and management bridge open)	15 minutes	ASAP (1-4 hours)
Severity 2 (P2)	High	Yes (Notification via Service Desk and tech bridge open)	30 minutes	8 hours
Severity 3 (P3)	Medium	No (updates in the ticketing system)	1 hour	3 Business Day
Severity 4 (P4)	Low	No (updates in the ticketing system)	2 hours	5 Business Days

## What are the business responsibilities?

---

- Report any issues as soon as possible through the Minnesota Service Hub or by contacting the MNIT Enterprise Service Desk.

- To make sure the application and any changes to the application is coordinated with the MNEIAM team to ensure uninterrupted service.

## **When will regular maintenance be performed?**

---

- MNEIAM Architects will work collaboratively with the Linux server team to devise an agreed upon schedule for regular maintenance of Identity Access Management servers, with consideration not to impact the agency's systems at the time of the maintenance window. If any exceptions occur and the maintenance window must be rescheduled, approval from MNIT Enterprise must be obtained and MNIT Enterprise will then relay to the applications. If necessary, an exception form will be submitted to the MNIT Enterprise Security team to reschedule the regular maintenance window.

## **Change Management Process/Termination**

---

- Any change management process/termination will be discussed in collaboration with the MNEIAM management team, the MNEIAM architect, and the agency's business and technical liaisons by preparing a communication plan to review and execute needed a mode of IAM operations and integrations.

# Service Name: Web Management Services

Revision Date 09/15/2021

## Executive Summary

Service Details	Summary Description
Service Name	<a href="#">Web Management</a>
Included	<ul style="list-style-type: none"> <li>Enterprise Web Content Management - SDL Web (Tridion) and Hosting</li> <li>Website development, design, and support</li> </ul>
NOT included	<ul style="list-style-type: none"> <li>Customer application support</li> <li>Optional: Quality Assurance website tool and Web Analytics</li> </ul>
Delivery Method	<ul style="list-style-type: none"> <li>Fulltime support staff with access to MNIT on-premise and external cloud environments</li> </ul>
Hours of Operation	<ul style="list-style-type: none"> <li>Production availability 7x24x365</li> </ul>

## Description

MNIT's Web Management Services refers to the inventory, development, and innovation of state websites as an asset to the overall digital estate. This includes:

- Website hosting and lower environments
- Website development and design
- Web Content management tools
- Search and website platforms, templates, and customizations
- Chatbot capabilities
- Interactive, lightweight applications and forms
- Multi-lingual, natively accessible, secure websites

Note: MNIT support of quality assurance and analytics tools is limited to those tools offered by the service.

As part of the Web Management service, MNIT offers an enterprise web content management system (WCMS) SDL Web (Tridion) and web hosting options. Our WCMS hosts the MN.gov portal and the Governor's Office Website, which includes 188+ supported sites supported with capacity for more.

## What systems or services are supported?

---

- Enterprise web content management system SDL Web (Tridion) and its hosting environments
- Static websites and hosting

## What services are included?

---

- **Staging and live publishing environments for both dynamic and static web options:**
  - **Full-Service Enterprise Web Content Service Management** – Enterprise content management services that allows state employees to build, launch and maintain their own websites. This may include templates, training, user group, hosting, support services, monitoring, security, usage reporting, disaster recovery, identity and access management, licensing, site health monitoring, etc.
  - **Static Web Hosting (HTML, ASP, etc.)** – Allows customers to host their own content and multi-media content (internal or vendor provided).
- **Robust environments and support including:**
  - Enhanced security protections
  - Accessibility standards that meet WCAG 2.0 standards and ARIA recommendations
  - Load balancing
  - Environment redundancy and fail over
  - Backup and recovery (full DR Plan)
  - Enhanced monitoring tools for system health
  - Patches & upgrades of the WCMS
  - Website publication migration from one release to another (the content on the website is responsibility of the agency)
  - Software version control for enhancements

## What services are NOT included?

---

- Management and use of the business side application
- Content management
- WCMS Website Publication license and Content Management user licenses
- Optional Web Management services provided at an additional cost:
  - **Quality Assurance website tool**
    - Includes scheduled or on-demand reporting of accessibility, link checking and spellcheck
  - **Web Analytics**
    - Advanced website statistics including user journeys, conversion rates and A/B testing
    - Visualization of users' clicks and scrolls with heat maps
    - Priority pages, referral paths and demographics of users

- Feedback mechanism, create workflows and respond to users in real time
- **Custom Search**
  - Search capabilities outside of the WCMS in Static Web Hosting
- **Chatbot**
  - Dynamic chatbots with usage reports can link to live agents
- **Professional Services**
  - A service agreement is required for one-time professional services charges for website development, design, content migration, search customization, and any further customizations. These costs are separate from the monthly hosting costs. Professional Services available include:
    - Initial environment configuration
    - Branding and design, within enterprise templates
    - Information architecture
    - WCMS training and support
    - Content management
    - Customized configuration of search capability and tuning
    - Customized templates for the agency website
    - Customized configuration of analytics tracking codes
    - API integration with existing applications

## How will the service be delivered?

---

- Fulltime support staff
- Either from the MNIT on premise or external cloud computing environment, depending on the business needs or requirements

## What are the hours of operation and how to get support?

---

- Production availability 7x24x365
- Service hours for Web Management support services:
  - WCM support hours: M-F; 7 a.m.-5 p.m. (except holidays)
  - On-call support is not available
- Submit requests through the online Minnesota Service Hub
- Submit break/fix incidents through the MNIT Service Desk



## What will the response time be?

Response Level	Definition	Example	Response Target	Return to Service Target
Priority 1 Critical	<p>The hosted website is not operational for multiple users, or citizens during scheduled availability</p> <p>A major function of the hosting service is not operational for multiple users during the hours that the service is scheduled for availability</p>	Site displays a 500 Internal Server Error	15 minutes*	2 hours*
Priority 2 High	<p>A user needs administrative assistance performing urgent updates or maintenance</p> <p>A minor function of the hosting service is not operational for many users (who can continue to use other application functions)</p>	Web content managers are unable to access WCMS or static site folders to update security related issues, contents, and site functionality	2 hours*	4 hours*
Priority 3 Med	<p>A user has questions about the hosting service functionality or needs assistance in using the service</p> <p>A minor function of the hosting service is not operational for one or few users (who can continue to use other application functions)</p>	Web content managers are unable to access WCMS or static site folders to update low priority contents and verbiage	8 hours*	8 hours*
Priority 4 Low	The hosting service is not operational for one or few users outside of the hours of availability – and is not impacting citizen facing services or sites	One person reports issue with their browser displaying page content.	2 business days	2 business days

\* Times listed represent normal business hours 7:00AM-5:00PM, as this service does not have on-call support

## What are the business responsibilities?

---

All installations are subject to a design process between MNIT and the subscriber. This process will ensure the subscriber's needs are met while adhering to MNIT Managed Hosting design requirements.

The customer is responsible for the following:

- Submit requests through the online MNIT Service Hub
- Requests for new website
- Provide a detailed requirements document
- Requests for decommissioning of old websites
- Requests for modifying websites
- Submit break/fix incidents through the MNIT Service Desk
- Provide resources to perform systems testing as needed
- Provide customer contact information, customer number and charge number

## When will regular maintenance be performed?

---

- As updates and patches are provided from the software vendor
- Any updates are planned, scheduled and performed within the existing change management windows

## Change Management Process/Termination

---

- MNIT follows established enterprise change management procedures and processes

# Service Name: Laptop/Desktop Bundle

Revision Date 07/14/2021

## Executive Summary

Service Details	Summary Description
Service Name	<a href="#">Laptop Bundle/Desktop Bundle</a>
Included	<ul style="list-style-type: none"> <li>• Standard Laptop, replaced every 4 years</li> <li>• Standard Desktop, replaced every 5 years</li> <li>• Docking station, keyboard and mouse (replaced with laptop if necessary, monitor not included)</li> <li>• Workstation management and protection package: security patching and encryption</li> <li>• Workstation support, including remote desktop and deskside support.</li> <li>• Inventory management</li> </ul>
NOT included	<ul style="list-style-type: none"> <li>• Performance-upgraded laptop/desktop</li> <li>• Monitor(s)</li> <li>• Memory upgrade</li> <li>• Headset</li> <li>• Cameras (required to use all the functionality of Microsoft Teams)</li> <li>• Local printer, if applicable for your agency</li> <li>• Ergonomic or wireless bundle for keyboard and mouse</li> <li>• Programmable keyboard</li> <li>• Shorter refresh cycle (see details below)</li> </ul>
Delivery Method	<ul style="list-style-type: none"> <li>• Fulltime staff for both remote and deskside support</li> </ul>
Hours of Operation	<ul style="list-style-type: none"> <li>• 24x7x365 with following hours of support:</li> <li>• M-F; 7 a.m.-5 p.m.</li> </ul>

## Description

Bundles include standard laptop and desktop computers selected from the list of Enterprise Standard devices adopted by MNIT Services, plus workstation management, support, and inventory management

of hardware and software. Standard laptops and desktops are selected from the list of Enterprise Standard devices adopted by MNIT Services.

Upgrade options are available to meet business needs. There is a one-time charge at the time of purchase for optional add-ons and hardware upgrades (listed below). Monthly bundle rates will remain unchanged.

### **Considerations**

- Billing details: Invoicing is based on monthly usage counts that are downloaded from the BMC Helix Configuration Management Database (CMDB). Only devices in a “Deployed” status are billable.
- Agency partners purchasing Laptop/Desktop Bundles must also purchase Enterprise Software Bundles.
- Hardware will be replaced every 4 years for laptops and 5 year for desktops unless the agency requests and pays for a shorter replacement cycle. Longer replacement cycles are not allowed.
- Shorter refresh cycles of 2-3 years are available (a one-time charge will apply) but must be applied to all laptop/desktop bundles at the agency.
- Early replacement of individual laptops/desktops requires the agency to pay off the remaining months of the life expectancy of the device.

### **What systems or services are supported?**

---

- Laptop/Desktop PC's
- Monitors
- Keyboard and mouse
- Security patching and encryption
- Inventory management for hardware and software

### **What services are included?**

---

- Workstation management and protection package
- Workstation support, including remote desktop and desktide support

### **What services are NOT included?**

---

- WAN Management

- Firewall configuration

## **How will the service be delivered?**

---

- Fulltime Support Staff
- Remote and Deskside configuration

## **What are the hours of operation and how to get support?**

- 7x24x365 up time with following support hours - M-F, 7 a.m.-5 p.m.
- Submit requests through the Minnesota Service Hub – Desktop/Computer Support
- Submit break/fix incidents through the MNIT Service Desk

## What will the response time be?

Response Level	Definition	Example	Response Target	Return to Service Target
Priority 1 Critical	Interruption making a critical functionality inaccessible or a complete interruption causing a severe impact on public-facing services availability.	All users at an agency are unable to log into the network causing an impact to public services.	30 minutes	*Immediately
Priority 2 High	Critical functionality or accessibility interrupted, degraded or unusable, having a severe impact on internal services availability. No acceptable alternative is possible.	Users are unable to access a critical application; the impact is limited an individual agency.	1 hour	12 hours
Priority 3 Medium	Non-critical function or procedure, unusable or hard to use having an operational impact, but with no direct impact on services availability. A workaround is available.	Email encryption is intermittently failing	24 hours	72 hours
Priority 4 Low	Application, procedure, or peripheral device is unusable for an individual user.	A user's docking station or external monitor is not functioning.	48 hours	120 hours

\*Note: Priority 1 service interruptions receive the highest priority and are given immediate attention until the issue is resolved. The goal is to restore functionality as soon as possible.

## What are the business responsibilities?

- Request or discontinue services and devices by submitting onboarding/off-boarding tickets through the Minnesota Service Hub
- Submit Minnesota Service Hub tickets for moves, adds, changes and incident support
- Provide information to assist with incident and work order resolution

## **When will regular maintenance be performed?**

---

- As updates and patches are provided from the equipment manufacturer or software provider
- Any updates are planned, scheduled and performed within the existing change management windows

## **Lost, stolen or damaged equipment caused by negligence**

---

This is the responsibility of the agency.

## **Change Management Process/Termination**

---

MNIT Services follows established enterprise change management procedures and processes.

# **Service Name: Enterprise Security Services**

**Revision Date 09/14/2021**

## **Executive Summary**

---

Enterprise Security Services are provided to all MNIT Services Executive Branch customers at a core level. These services are offered and supported by dedicated teams which include: Security Operations Center (SOC), Enterprise Threat and Vulnerability Management, Access and Identity Management (broken down below into Enterprise Privileged Account Management Service and Enterprise Digital Certificate and Encryption Key Management), Digital Forensics, Secure Engineering and Architecture (SEA) and Governance, Risk, and Compliance. Within each of these teams, additional protective services are provided and listed below.



## Enterprise Threat and Vulnerability Management

---

Service Details	Summary Description
Service Name	Enterprise Threat and Vulnerability Management
Included	<ul style="list-style-type: none"> <li>• Internal Vulnerability Scanning of desktops, servers, network devices and other supported devices</li> <li>• External scanning of internal facing devices</li> <li>• Communication of prioritized vulnerabilities</li> <li>• Oversight of remediation efforts on vulnerabilities</li> <li>• Configuration compliance scanning (emerging capability)</li> <li>• Web application security scanning (DAST)</li> <li>• Veracode administration for teams using Veracode static code analysis tool (SAST) <ul style="list-style-type: none"> <li>○ Dedicated subject matter expert to assist with taking full advantage of Veracode</li> </ul> </li> <li>• In-depth web application security assessment (upon request)</li> <li>• Cloud Web Application Firewall (WAF) and Bot service administration</li> <li>• Penetration and Red Team Services (emerging capability)</li> </ul>
NOT included	<ul style="list-style-type: none"> <li>• Devices not connected to MNIT managed networks</li> <li>• Devices not supported by TVMU tools</li> </ul>
Delivery Method	<ul style="list-style-type: none"> <li>• Fulltime support Staff</li> <li>• Automated scanning</li> <li>• MNIT Mall: Threat and Vulnerability Management</li> </ul>
Hours of Operation	<ul style="list-style-type: none"> <li>• M-F; 7 a.m.-5 p.m.</li> <li>• Emergency after hours support: MNIT Service Desk</li> </ul>

## Security Operations Center (SOC)

---

Service Details	Summary Description
Service Name	Security Operations Center
Included	<ul style="list-style-type: none"> <li>• Security Incident Response</li> <li>• SOC Daily Briefing – informed by Threat Intelligence</li> <li>• Spam/Phishing Investigation</li> <li>• Security Operations Coordination</li> <li>• Security Monitoring</li> <li>• Enterprise Intrusion Detection and Prevention</li> <li>• Enterprise Web Content Filtering</li> <li>• Enterprise Endpoint Protection</li> <li>• SIEM (log collections) <ul style="list-style-type: none"> <li>○ Threat Hunting</li> </ul> </li> <li>• Threat Intelligence</li> <li>• Distributed Denial of Service (DDOS) attack protection</li> <li>• Netflow monitoring and detection for all MNet networks</li> </ul>
NOT included	<ul style="list-style-type: none"> <li>• Full service provided to MN executive branch and partner entities with core detection/alerting to other MNET customers</li> <li>• Monitoring is limited to network activity only for external MNET entities that do not participate in the Intrusion Detection and Prevention Service</li> </ul>
Delivery Method	<ul style="list-style-type: none"> <li>• Fulltime support staff</li> <li>• Email: <a href="mailto:soc@state.mn.us">soc@state.mn.us</a></li> <li>• Phone: 651.201.1281</li> <li>• MNIT Mall: Report a Security Event</li> </ul>
Hours of Operation	<ul style="list-style-type: none"> <li>• Daily 6 a.m. – 6 p.m.</li> <li>• Emergency after hours support: MNIT Service Desk 24x7</li> <li>• Overwatch (365/24x7) endpoint monitoring</li> </ul>

## Digital Forensics

---

Service Details	Summary Description
Service Name	Digital Forensics
Included	<ul style="list-style-type: none"> <li>• Security Incident Investigations               <ul style="list-style-type: none"> <li>○ Data breach incident</li> <li>○ Malware/Ransomware incident</li> <li>○ Intrusion incident</li> </ul> </li> <li>• Forensics case consultation</li> </ul>
NOT included	<ul style="list-style-type: none"> <li>• Devices not owned by executive branch agencies*</li> </ul>
Delivery Method	<ul style="list-style-type: none"> <li>• Fulltime support staff</li> <li>• MNIT Mail: Use the Agency Data &amp; Legal Hold Request Form</li> <li>• Email: mnit.forensics@state.mn.us</li> <li>• Phone: 651-201-3067</li> </ul>
Hours of Operation	<ul style="list-style-type: none"> <li>• M-F: 8 a.m. to 4:30 p.m. CST</li> <li>• Emergency after hours support: MNIT Service Desk 24x7</li> </ul>

*\* Exceptions made upon specific incident investigation request*

## Secure Engineering and Architecture

---

Service Details	Summary Description
Service Name	Secure Engineering and Architecture
Included	<ul style="list-style-type: none"> <li>• Set the direction for Minnesota's security architecture through:               <ul style="list-style-type: none"> <li>○ Development of technical security configuration and technical reference architecture standards</li> <li>○ Integrating secure design principles and processes into MNIT Services projects and initiatives</li> <li>○ Portfolio management and systems &amp; applications development processes</li> </ul> </li> <li>• Provide Security Architect and Engineering consulting resources to enterprise projects and initiatives</li> <li>• Operate a Payment Card Industry (PCI) program to monitor state compliance and secure Cardholder Data Environments (CDE)</li> <li>• Provide security and compliance consulting services for agency PIC compliance</li> <li>• Operate vender security risk management services to executive branch.</li> </ul>
NOT included	LOB team security consulting
Delivery Method	<ul style="list-style-type: none"> <li>• Fulltime support staff</li> <li>• Email: sse@state.mn.us</li> </ul>
Hours of Operation	<ul style="list-style-type: none"> <li>• M-F: 8 a.m. to 4:30 p.m. CST</li> </ul>

## Enterprise Privileged Account Management Service

---

Service Details	Summary Description
Service Name	Enterprise Privileged Account Management Service
Included	<ul style="list-style-type: none"> <li>• User license</li> <li>• Centralized, secure storage</li> <li>• Automatic password rotation</li> <li>• Automated Workflows</li> <li>• Security Awareness training</li> <li>• Access oversight and audit</li> <li>• Connection manager</li> </ul>
NOT included	<ul style="list-style-type: none"> <li>• Storage of personal passwords</li> </ul>
Delivery Method	<ul style="list-style-type: none"> <li>• Fulltime Support staff</li> <li>• MNIT Mall: Privileged Account Access</li> </ul>
Hours of Operation	<ul style="list-style-type: none"> <li>• M-F; 7 a.m.-5 p.m.</li> <li>• Emergency after hours support: MNIT Service Desk</li> </ul>

## Enterprise Digital Certificate and Encryption Key Management (PKI)

---

Service Details	Summary Description
Service Name	Enterprise Digital Certificate and Encryption Key Management (PKI)
Included	<ul style="list-style-type: none"> <li>• Management of external digital certificates</li> <li>• Management of internal digital certificates</li> </ul>
NOT included	<ul style="list-style-type: none"> <li>• Management of encryption keys</li> </ul>
Delivery Method	<ul style="list-style-type: none"> <li>• Fulltime Support staff</li> <li>• MNIT Mall: Security Certificates</li> </ul>
Hours of Operation	<ul style="list-style-type: none"> <li>• M-F; 7 a.m.-5 p.m.</li> <li>• Emergency after hours support: MNIT Service Desk</li> </ul>

## Enterprise Governance, Risk, and Compliance

---

Service Details	Summary Description
Service Name	Enterprise Governance, Risk, and Compliance
Included	<ul style="list-style-type: none"> <li>• Develop/update Minnesota's State Security Policies and Standards</li> <li>• Maintain/manage the Archer application (RSA tool that helps us provide an integrated picture of security risk)</li> <li>• Custodian of agency security findings and exceptions in Archer</li> <li>• Provide support to agencies for audits/assessments that have IT security compliance requirements</li> <li>• Conduct IT security risk assessments on applications and systems</li> <li>• Partner with MNIT Communications to provide monthly security awareness messaging and October Cyber Security month awareness messaging</li> <li>• Partner with vendor to ensure security awareness training is delivered to agency staff</li> <li>• Partner with vendor to ensure that monthly phishing campaigns are sent to agency staff and that agencies receive monthly reports</li> <li>• Security Scorecard Metrics process oversight</li> </ul>
NOT included	
Delivery Method	<ul style="list-style-type: none"> <li>• Fulltime support staff               <ul style="list-style-type: none"> <li>○ Email: <a href="mailto:GRC@state.mn.us">GRC@state.mn.us</a></li> </ul> </li> </ul>
Hours of Operation	<ul style="list-style-type: none"> <li>• M-F, 8 a.m.-5 p.m.</li> </ul>

## Description

---

### Enterprise Threat and Vulnerability Management

The Enterprise Vulnerability Management service provides the means of detecting, removing, and controlling the inherent risk of vulnerabilities. The service utilizes specialized software and insight to provide actionable insight into security risks and guidance on mitigating or eliminating these risks through ongoing evaluation, analysis, and tracking of enterprise systems and applications. A live dashboard is available to CBTOs and their teams tracking active vulnerabilities and agency compliance with Enterprise patching standards.

### Security Operations Center

The Security Operations Center (SOC) is an organized and highly skilled team whose mission is to continuously monitor and improve the state's enterprise security posture while preventing, detecting, analyzing, and responding to cybersecurity incidents with the aid of both technology and well-defined processes and procedures. The MNIT SOC provides security monitoring services to the executive branch and other partner agencies/entities and supports multiple tools and services to meet these goals. These services include Security Monitoring, Endpoint Protection, Network Intrusion Detection and Prevention, Security Automation, Web Content Filtering, SIEM (log collections and threat hunting), Threat Intelligence, Distributed Denial of Service (DDOS) attack protection, Volumetric and Web Application Firewall (WAF) monitoring, as well as Netflow monitoring and detection for all MNet networks. MNIT SOC provides cyber security analysis and statewide cyber security coordination to the Minnesota Fusion center. MNIT SOC provides additional security services to local governments through grants and other alternative funding streams.

### Digital Forensics

Digital forensics is the scientific process of acquiring, processing, analyzing, and reporting on data stored on electronic media or transmitted through electronic means such as computer networks. MNIT operates a Digital Forensics Laboratory which employs industry standard practices, processes, procedures, and tools. MNIT Forensics procedures include maintaining a chain-of-custody and following forensically sound processes whenever possible. MNIT Forensics engages in a wide variety of analysis to include, but not limited to, physical media (such as hard drives), smartphones, network devices, malware, system logs, live system memory (RAM), and virtual machines (VMs). MNIT Forensics performs cybersecurity investigations as well as internal investigations. In addition to investigations, MNIT Forensics manages the Enterprise eDiscovery Service.

### Secure Engineering and Architecture

Secure Engineering and Architecture (SEA), a function of Enterprise Architecture, proactively engages IT engineers, architects and developers to design security controls into IT systems and applications early in the development lifecycle. The focus of SEA is to ensure purchased, outsourced, or internally



developed IT systems and applications are designed and implemented to meet the State of Minnesota's security architecture and secure coding standards.

### **Enterprise Privileged Account Management Service**

The Enterprise Privileged Account Management (PAM) service is designed to discover, secure, rotate and control access to privileged account passwords used to access systems throughout the state of Minnesota IT environment. The application enables us to understand the scope of our privileged account risks and put controls in place to mitigate those risks. Flexible password management policies enable us to enforce privileged access controls, automate workflows and rotate passwords at regular intervals without requiring manual IT effort to support our Enterprise Identity and Access Management Standard. To demonstrate compliance, we can easily report on which users accessed what privileged accounts, when and why.

### **Enterprise Digital Certificate and Encryption Key Management (PKI) Service**

A public key infrastructure (PKI) is a set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption. The PKI service provides security services such as authentication, integrity checking, confidentiality, and non-repudiation, as well as supports the identification and distribution of encryption keys.

The PKI service includes both external and internal digital certificates issued by a commercially available, industry-respected vendor. External certificates use a broadly distributed, public certificate authority (CA) meaning most or all internet connected devices can use these certificates without special configuration. Internal certificates use an enterprise certificate authority (CA) unique to the state of Minnesota and will only work between machines that have that CA specifically installed. Generally, external certificates are used on websites facing the public or large populations of state employees. Internal certificates are more common between backend servers, devices, and machine certificates for remote access for unregulated two-factor authentication.

### **Enterprise Governance, Risk and Compliance**

Governance, Risk, and Compliance (GRC) plays a key role in MNIT's strategy to reduce IT security risk.

- Governance - develop and update Security Policies and Standards that support organizational goals.
- Risk - manage information security findings/exceptions in RSA Archer, which helps provide an integrated picture of IT security risk.
- Compliance - help ensure that IT systems, and the data contained in those systems are used and secured properly, to meet legal and regulatory requirements.

## What systems or services are supported?

---

### Security Operations Center and Digital Forensics

- All enterprise networks, systems, services, and applications

### Privileged Account Management Service

- Available services are based on user's license.
- Users are in the appropriate OU within Active Directory.
- Active Directories are synced with privileged account management solution.
- Service Account password rotation
- Recertification of users of information technology.

### Enterprise Digital Certificate and Encryption Key Management (PKI) Service

- Commercial Certificate Authority (CA) at an enterprise level providing for unlimited external digital certificates.
- State managed Enterprise Certificate Authority (CA) for unlimited internal digital certificates.
- Managed expiration dates with 90/60/30 day notification to technical teams.
- Automation of certificate replacement
- FIPS 140-2 Compliant.
- Various certificate types:
  - Elite SSL Certificate
  - Extended Validation (EV) SSL Certificate
  - Platinum Wildcard Certificate
  - Unified Communication\Multiple Domain\Subject Alternative Domain Certificate
  - Code Signing Certificate
  - Private Certificate Authority (CA) Certificate
- Various certificate formats
  - PKCS#7 Base64 encoded
  - PKCS#7 Bin encoded
  - X509, Base64 encoded
  - X509 Certificate only, Base64 encoded
  - X509, Intermediates/root only, Base64 encoded
  - X509 Intermediates/root only Reverse, Base64 encoded

## What services are included?

---

### Enterprise Threat and Vulnerability Management

- Full Internal vulnerability scanning with credentials using Tenable Security Center against the following MNIT Managed systems on MNIT wired and wireless networks
  - Windows Desktops
  - Windows Servers
  - Networking devices
  - Linux servers
  - Cloud (AWS, Azure) servers
  - Virtual Infrastructure devices
- Limited vulnerability scanning using Tenable Security Center against all other networked devices (where scanning has vulnerability coverage). These devices may include:
  - Printers
  - IoT devices, such as cameras
  - Appliances
  - Industrial Control devices
- External Vulnerability scanning against MNIT managed internet facing devices.
- Prioritized communication of vulnerability scan results to technical operation teams.
- Oversight of remediation effort by technical support teams.
- Configuration Compliance Scanning for the MNIT approved platform security standards against MNIT data center servers and any regulatory platform security standard, such as the IRS Federal Tax Information (FTI).
- Web applications security scans.
- Veracode administration for teams using Veracode.
  - Dedicated subject matter expert to assist with taking full advantage of Veracode (SAST)
- In-depth web application security assessment upon request (DAST)
- Cloud Web Application Firewall (WAF) and Bot service administration
- Managed Penetration and Red Team Services through third-party contractor.

### Security Operations Center

- Security Incident Response
- Threat Research and SOC Daily Brief
- Spam/Phishing Investigation
- Security Operations Coordination
- Security Monitoring
- Enterprise Intrusion Detection and Prevention
- Enterprise Web Content Filtering

- Enterprise Endpoint Protection
- SIEM (log collections)
  - Threat Hunting
- Threat Intelligence
- Distributed Denial of Service (DDOS) attack protection
- Netflow monitoring and detection for all MNet networks

## **Digital Forensics**

- Security Incident Investigations
  - Data breach incident
  - Malware/Ransomware incident
  - Intrusion incident

## **Privileged Account Management Service**

- User license
- Centralized, secure storage
- Automatic password rotation
- Automated Workflows
- Security Awareness Training
- Access oversight and audit
  - Detailed auditing and reporting as all account activity is tracked and recorded
  - Data access security monitoring
  - Recertification of user access

## **Enterprise Digital Certificate and Encryption Key Management (PKI) Service**

- Commercial certificate authority (CA) license and support for unlimited external digital certificates
- Enterprise State managed certificate authority (CA) for internal certificates
- Management of the digital certificates
- Security Awareness training
- Vulnerability management on the State certificate authority

## **What services are NOT included?**

---

### **Enterprise Threat and Vulnerability Management**

- Vulnerability management of MNIT-managed devices not connected to MNIT wireless and wired networks
- Vulnerability management of devices that are not covered by TVMU vulnerability scanning tools.

## Security Operations Center

- Full service provided to Minnesota executive branch and partner entities with core detection/alerting to other MNET customers
- Monitoring is limited to network activity only for external MNET entities who do not participate in the Intrusion Detection and Prevention Service

## Digital Forensics

- Devices not owned by executive branch agencies\*
- Internal investigations
- Data Preservation
- Data Recovery
- eDiscovery

*\* Exceptions made upon specific incident investigation request*

## Privileged Account Management Service

- The current service does not provide a self-service password reset. This feature may be added in the future.
- This service does not provide personal password management.

## Enterprise Digital Certificate and Encryption Key Management (PKI) Service

- The current service does not provide management of encryption keys. This is planned future enhancement.
- Discovery of digital certificates
- The service does not provide a self-service portal.

## How will the service be delivered?

---

- Fulltime support staff

## What are the hours of operation and how to get support?

---

- Submit requests through the MNIT Mall – Service Catalog.
- Submit break/fix incidents through the MNIT Service Desk.
- MNIT support M-F; 7 a.m.-5 p.m.
- Emergency after hours support through MNIT Service Desk.

See specific team description above for service-related support hours.

## What are the business responsibilities?

---

- Business assumes risks associated with unsupported applications with vulnerabilities.
- The business agrees to regular update and patching maintenance of supported business system and applications.

### Privileged Account Management Services

- Order on-boarding/off-boarding through the MNIT Mall.
- Submit MNIT Mall tickets for moves, adds, changes and incident support.
- Provide application information support to assist with incidents and work orders.

### Enterprise Digital Certificate and Encryption Key Management (PKI) Service

- Submit MNIT Mall tickets for adds and revokes and incident support.
- Provide information support to assist with incidents and work orders.

## When will regular maintenance be performed?

---

- As updates and patches are provided from the equipment manufacturer or software provider.
- Any updates are planned, scheduled, and performed within the existing change management windows.

## Change Management Process/Termination

---

MNIT follows established enterprise change management procedures and processes.

# Service Name: Enterprise Software Bundles

Revision Date 07/15/2021

## Executive Summary

Service Details	Summary Description
Service Name	<a href="#">Enterprise Software Bundle</a>
Included	<p><b>Bundle Options:</b></p> <ul style="list-style-type: none"> <li> <b>Standard Bundle - NEW</b>            An all-inclusive option that enables knowledge workers to take advantage of the most advanced Microsoft feature sets with no need to purchase additional licenses for Power BI Pro and the Audio-Conferencing add-on.           <ul style="list-style-type: none"> <li> <b>Power BI Pro</b> is an analytic tool that can transform your business by turning data into useful information. Data models, visualizations, charts, graphs and trend analysis will provide new insights into your organization to improve strategic planning and tactical initiatives.             </li> <li> <b>Audio-Conferencing Add-on</b> for MS Teams users is a great option for project managers or anyone who regularly schedules or hosts on-line video and voice enabled meetings. It includes both dial-in and dial-out numbers facilitating easy conferencing meeting participation. This cost-effective option may eliminate the need for a separate service for some users.             </li> <li> <b>Microsoft Cloud App Security</b> is included in this bundle. Agencies can determine how these enhanced security features work best with their local business processes.             </li> </ul> </li> <li> <b>Basic Bundle</b>            Most office workers in today's environment have basic communication and collaboration needs that are served by the components in this Enterprise Software Bundle including Email, Office, Windows, Teams and SharePoint. Most state workers currently use this bundle.         </li> </ul>

	<ul style="list-style-type: none"> <li>• <b>Kiosk</b>  This bundle is designed for groups of employees who share a single device. It is a good option for people who only need a computer for time entry, agency intranet access, checking email, calendars and Office online use. It includes a SharePoint access license and Teams licensing to support collaborative team activities.  This does not include features for the devices so Windows licensing and the installed Office client will need to be purchased separately for each shared machine.</li> <li>• <b>Education Bundle</b>  This is a version of MNIT's "Basic Bundle" that is available only for educational organizations and is priced according to Microsoft educational discounts. It does not provide Microsoft Windows or Office Client licensing.</li> <li>• <b>Exchange Online Only – NEW</b>  This bundle is restricted for use by applications and servers only. It is often referred to as a Service Agent license or Non-human license and is for agencies who have business applications that automatically send emails to users.</li> </ul>
NOT included	<ul style="list-style-type: none"> <li>• Agency-specific software packages</li> </ul>
Delivery Method	<ul style="list-style-type: none"> <li>• Fulltime support staff for both online and desktide support.</li> </ul>
Hours of Operation	<ul style="list-style-type: none"> <li>• Access to Foundational Services (Email, SharePoint and Teams) 24x7x365 from Microsoft</li> <li>• Following hours of Minnesota IT Services support. M-F, 7 a.m.5 p.m.</li> </ul>

## Description

---

State workers in today's environment have basic communication and collaboration needs that can be served by Enterprise Software Bundles, including email, instant messaging and enhanced collaboration tools. At the same time MNIT has recognized the need for additional options for users requiring specific Microsoft add-ons. There has also been a recognition for the need of a low-cost license for service accounts.

## What systems or services are supported?

---

### Workstation Services and Rates (Core Service)

Standard and Basic Workstation Bundles are billed monthly, and include the following:



- Microsoft Office 365: Word, Excel, PowerPoint, Outlook, OneNote, Access
- Microsoft Windows license
- SharePoint license
- Teams
- Security awareness training
- Access oversight and audit
  - Physical access to data centers and data
  - Data access security monitoring

The Education Bundle does not include Microsoft Windows or the installed client for Microsoft Office.

### **Kiosk Worker Services and Rates (Core Service)**

This bundle is useful in situations where many people share the use of a single computer for tasks such as time entry, accessing the agency intranet or checking email or calendars. All Kiosk services include the following:

- Microsoft Office 365, Kiosk User Office Online
- SharePoint access license
- Security awareness training
- Teams
- Access oversight and audit
  - Physical access to data centers and data
  - Data access security monitoring

### **Exchange only**

This is a service account license for machines running applications that need automated email services.

## **What services are included?**

---

Available services are based on user's license.

## **What services are NOT included?**

---

Agency specific software must be purchased separately.

## **How will the service be delivered?**

---

- Fulltime support staff
- Remote and deskside configuration

## What are the hours of operation and how to get support?

---

### Minnesota IT Services Service Desk Contacts

**Business Hours:** 24 x 7  
**Contact Name:** Minnesota IT Services Service Desk  
**Phone Number:** 651-297-1111  
**Website and Service Catalog:** [mn.gov/MNIT](http://mn.gov/MNIT)

- Submit requests through the Minnesota Service Hub
- Submit break/fix incidents through the MNIT Service Desk
- Email service support provided by MNIT Services is delivered M-F, 7 a.m. - 5 p.m.
- SharePoint service support provided by MNIT Services is delivered M-F, 7 a.m. – 5 p.m.
- MS Teams service support provided by MNIT Services is delivered M-F, 7 a.m. – 5 p.m.
- Foundational services (Email, SharePoint and Teams) hosting and support is provided by Microsoft 24x7x365

## What will the response time be?

---

Response Level	Definition	Example	Response Target	Return to Service Target
Priority 1 Critical	An Issue that results in a critical business impact for a Production System.	All users are unable to log into network	15 Min	2 hours
Priority 2 High	An Issue that results in a high business impact for a Production System or Development System. Certain functions within the software are disabled, but the Software remains operable.	Developers are unable to access a feature of an application	2 hours	8 Hours
Priority 3 Med	A time-sensitive Issue important to long-term productivity that is not causing an immediate work stoppage.	Email encryption is intermittently failing	8 Hours	2 days
Priority 4 Low	An Issue that results in a minimal business impact for a Production System or Development System.	A specific font is not available for a user.	5 Days	10 days

## **What are the business responsibilities?**

---

- Order on-boarding/off-boarding through the Minnesota Service Hub.
- Submit tickets for moves, adds, changes and incident support through the Minnesota Service Hub.
- Provide information support to assist with incidents and work orders.

## **When will regular maintenance be performed?**

---

- As updates and patches are provided from the equipment manufacturer or software provider.
- Any updates are planned, scheduled and performed within the existing change management windows.

## **Change Management Process/Termination**

---

Minnesota IT Services follows established enterprise change management procedures and processes.

# Service Name: Geospatial Shared Services

Revision Date 10/28/21

## Executive Summary

Service Details	Summary Description
Service Name	Geospatial Shared Services
Included	<ul style="list-style-type: none"> <li>Enterprise Licensing for Geospatial Software</li> <li>MN Geospatial Commons</li> <li>Access and use of geospatial web services</li> <li>Geospatial Managed Hosting</li> <li>Access to PT Services for development and support of geospatial applications and web services</li> </ul>
NOT included	
Delivery Method	<ul style="list-style-type: none"> <li>Fulltime support staff with access to the MNIT On-Premise and external cloud environments</li> </ul>
Hours of Operation	<ul style="list-style-type: none"> <li>Production availability 7x24x365</li> </ul>
Hours of Support	<ul style="list-style-type: none"> <li>7am-5pm Monday-Friday (except holidays)</li> </ul>

Minnesota IT Services' (MNIT) Geospatial Information Services office (MnGeo) provides shared geospatial services that support the development, implementation and use of geospatial technology to a wide variety of stakeholders in Minnesota. Guided by state agencies, other government and non-government stakeholders, these geospatial shared services focus on the access to geospatial data and technology through providing access to enterprise licensing and web services that can be incorporated into applications and web browsers.

MnGeo provides access to four types of shared services including enterprise GIS licensing, geospatial data hosting and portal, and web services. To use the services, customers can submit a service request or contact MnGeo at [gisinfo.mngeo@state.mn.us](mailto:gisinfo.mngeo@state.mn.us). A service agreement is required prior to the service being provided.

## What systems or services are supported?

---

- Geospatial enterprise software from Environmental Systems Research Institute and Microsoft (Bing Maps Services).
- Access to web and web map services.
- Publishing and access to the Minnesota Geospatial Commons.
- Geospatial managed hosting including Infrastructure as a Service (IaaS, Software as a Service (SaaS), and Platform as a Service (PaaS).
- Professional/Technical support services.

## What services are included?

---

### Enterprise Licensing for GIS Software

MnGeo administrates the state's enterprise license agreement with Environmental Systems Research Institute. Agencies are provided access to core GIS desktop and server software and online subscription tools and services at a significantly reduced rate. Key representatives are identified at each participating agency that can assist GIS professionals and business users with access to the software and services. MnGeo also serves as the key access point for obtaining GIS support. Learn more on [our website](#).

### Minnesota Geospatial Commons

The [Geospatial Commons](#) provides a hosted environment for agencies to publish geospatial data and metadata, and provides a common access point for agency or organization customers to access their data. Having data in a single place significantly reduces time for users to find and obtain the data.

### Web Services

MnGeo provides the following web services that agencies may obtain for use in applications, web pages. Technical documentation is available to agency customers:

- [Geocoding Service](#): MnGeo provides a secure "cascading" geocoding service for use in ArcGIS software and web applications. The service includes data layers for parcel points, address points, street centerlines, municipal boundaries, city centroids and 5 digit zip code centroids. The service is available only to State of Minnesota agencies for internal applications.
- [Bing Maps API](#): Access to the Bing Maps API can be requested by agencies. Each agency requesting access to the services is provided an "application key." The API can be used for both internal and external websites. The Bing Maps APIs include map controls and services that you can use to incorporate [Bing Maps](#) in applications and websites. In addition to interactive and static maps, the APIs provide access to other geospatial features such as geocoding, route and traffic data and spatial data sources that you can use to store and query data that has a spatial component, such as store locations. To learn more, see [Getting Started with Bing Maps](#).

## Geospatial Managed Hosting

Geospatial Managed Hosting is a service that uses services and storage in the State of Minnesota's enterprise data centers and secure cloud environment. This hosting service provides geospatial production, test, and development environments to deliver applications, data and services for customers. Requesting agencies may choose a shared or dedicated geospatial application hosting environment depending on their need.

Included in the service are: OS (operating system), geospatial software, professional services and underlying infrastructure support to assist application owners with configurations that meet application requirements.

## Professional Services

---

MnGeo offers a diverse set of GIS professional services to agencies on a fee-for-service basis. MnGeo staff work closely with its clients to define a suitable scope for the service, identify requirements, tasks and deliverables, create and refine a work plan and budget, execute and manage the defined effort to completion. All services are billed at monthly intervals.

## Contact us for more Information

---

For more information contact MnGeo [gisinfo.mngeo@state.mn.us](mailto:gisinfo.mngeo@state.mn.us).

## How will the service be delivered?

---

Fulltime support staff

## What are the hours of operation and how to get support?

---

- Service hours for Geospatial Managed Hosting and Web Services Support services:
  - Production availability 7x24 x365
  - Geospatial Support staff on premise 7am-5pm Monday-Friday (except holidays)
- Submit requests through the MNIT Mall - Service Catalog.
- Submit break/fix incidents through the MNIT Service Desk.

## What will the response time be?

Response Level	Definition	Example	Response Target	Return to Service Target
Priority 1 Critical	<p>The hosted website, application, or web service is not operational for multiple users, or citizens during scheduled availability</p> <p>A major function of the hosting service is not operational for multiple users during the hours that the service is scheduled for availability</p>	Site displays a 500 Internal Server Error	1 Hour	4 hours
Priority 2 High	<p>A user has questions about the hosting service functionality or needs assistance in connecting to or using the service</p> <p>A user needs administrative assistance performing urgent updates or maintenance</p> <p>A minor function of the hosting service is not operational for many users (who can continue to use other application functions)</p>	User need directions regarding how to connect to or use a service or application	4 hours	2 business days
Priority 3 Med	A minor function of the service or application is not operational for one or few users (who can continue to use other application functions)	Geocoding service not allowing batch updates	8 hours	3 business days
Priority 4 Low	The service is not operational for one or few users outside of the hours of availability – and is not impacting citizen facing services or sites	One person reports and issues with connecting to a service or using an application	2 business days	5 business days

## What are the business responsibilities?

---

All requests for new services or applications are subject to a design process between MNIT and the subscriber. This process will insure the subscriber's needs are met while adhering to MNIT Managed Hosting design requirements.

The customer is responsible for the following:

- Submitting requests for software or services or support through the MNIT Service Catalog.
  - If a new request for services, provide a detailed requirements document.
- Provide resources to perform systems testing as needed.
- Provide customer contact information, customer number and charge number.
- Submit requests for modifying applications or services through the MNIT Service Catalog.
- Submit break/fix incidents through the MNIT Service Desk.
- Submit requests for decommissioning of old websites through the MNIT Service Catalog.

## When will regular maintenance be performed?

---

- As scheduled or when updates and patches are provided from the software vendor.
- Any updates are planned, scheduled and performed within the existing change management windows.

## Change Management Process/Termination

---

MNIT follows established enterprise change management procedures and processes.



# Service Name: Voice

Revision Date 09/01/2021

## Executive Summary

---

Service Details	Summary Description
Service Name	<a href="#">Voice</a>
Included	<ul style="list-style-type: none"><li>Telephone service using state IP services or contracted traditional services</li></ul>
NOT included	<ul style="list-style-type: none"><li>Cellular Phones</li></ul>
Delivery Method	<ul style="list-style-type: none"><li>Dial tone to telephone handset and or softphone</li></ul>
Hours of Operation	<ul style="list-style-type: none"><li>24 x 7 x 365</li></ul>

## Description

---

Voice services provides business quality voice communications and a varied set of related features and capabilities. The service provides one telephone line in a state office, teleworker home office or other location.

## What systems or services are supported?

---

- A unique telephone number, voicemail, and a standard telephone handset (equipment)
- Long distance calling (outbound calling only, 1-800 type inbound long distance is additional)
- Microsoft Teams softphones
- Telecom coordination operational support
- Telephone equipment replacement on an as-needed basis

## What services are included?

---

- IP Telephone – A standard office IP telephone
- Basic Line - Telephone for specialized monitoring, faxing or equipment support purposes (no handset)
- Business Line - Phone service from a telephone company (when no Centrex services are available)

- Centrex Line - A specialized set of telephone services designed to provide much of the functionality of a private telephone system at a competitive price. Note: availability depends on the telephone company under contract for a particular location
- Softphone – Microsoft Teams integrated softphone functionality
- Small office Multi Line - An on-premise telephone system connected to telephone company trunk lines to support a small office
- Contact Center Agent service- A standard office IP telephone with a suite of contact center agent computer applications to support their work
- Contact Center Supervisor service- This service adds an additional set of capabilities for contact center supervisors to manage their team of agents

## What services are NOT included?

---

- Line installation fees from contracted telephony companies are billed as one-time charges
- Specialized phones (conference room speaker phones, etc.) are billed as one-time charges
- Specialized contact center services are billed separately, including but not limited to interactive voice response (IVR) applications; advanced contact center tools (quality management); workforce management applications
- Over-the-phone interpretation (OPI) and other language interpretation services.
- Audio conferencing and associated features, such as operator-assisted calls, and one-time audio conference services, such as audio recording files or transcriptions, are billed separately
- In-bound long distance toll service (1-800 services) is billed on a per minute basis
- Cellular services and phones

## How will the service be delivered?

---

Service requests to add, delete, or make feature changes are processed through the MNIT Service Desk. The MNIT Service Desk also maintains customer contact and account information. Customers can choose to use the Minnesota Service Hub website to submit requests.

Each MNIT customer has a designated Enterprise Relationship Manager who works with the customer on an individual basis for their IT service needs. In partnership with the Installation Coordinators and Service Managers, the Relationship Manager:

- Facilitates service implementation
- Coordinates MNIT staff and resources as needed
- Provides consultation, needs assessment, analysis, and cost-effective solutions
- Develops proposals and service agreements
- Assists with writing procurement specifications

## What are the hours of operation and how to get support?

---

### MNIT Service Desk Contacts

- **Business Hours:** 24 x 7 x 365
- **Contact Name:** MNIT Service Desk
- **Phone Number:** 651-297-1111
- **Website and Service Catalog:** [mn.gov/MNIT](http://mn.gov/MNIT)

## What will the response time be?

Response Level	Definition	Example	Response Target	Return to Service Target
Priority 1 Critical	Any Incident that has “massive impact” and is highly visible, impacts a significant number of users, a major agency, application or service, and has no redundancy or alternate path.	Dial Tone Services – telephone services for a large group of users are non-functional  Voice Related Services – a service is non-functional for all users	15 minutes	2 hours
Priority 2 High	Incident deemed to have a high impact by being highly visible, impacting a significant number of users, impacting a major agency, application or service, where there is no redundancy or alternate path, and a bypass is unavailable.	Dial Tone Services – telephone services for a group of users are non-functional  Voice Related Services – a service is non-functional for multiple users	2 hours	8 hours
Priority 3 Med	Incident deemed to have a medium impact by being visible, impacting a limited number of users, where a resource or service is down or degraded.	Dial Tone Services – telephone service for individual user is non-functional  Voice Related Services – a service for an individual user is non-functional	8 hours	2 business days
Priority 4 Low	Any incident that impacts a small number of users or a single user where a resource or non-critical service is down or degraded and a deferred fix or maintenance is acceptable.	Phone feature issue or voicemail problem	4 hours	5 business days

## What are the business responsibilities?

---

- Create, configure, and administer voice services specific to CUSTOMER site contact center agent users including features, functions, and other services and provide for any necessary documentation as needed and agreed to with MNIT (e.g., E911 location coding).
- Provide notification to MNIT of possible excessive demand for CUSTOMER contact center services that can potentially, significantly, and negatively impact state voice services administered centrally.
- Partner with MNIT to design, develop, test, implement, configure and/or modify all inbound and outbound contact center applications (per agent and supervisor licenses), workstations, and agent reports.
- Design, develop and test call authorization parameters (toll restrictions) and other network applications and work with MNIT to design, develop and implement reports and future network applications as needed.
- Provide to MNIT any necessary documentation as needed for acceptance and implementation on production system.
- Comply with established standards for design, development, testing, and implementation when developing new applications.
- Partner with MNIT to provide advanced contact center management features and applications.
- Provide workspace, funding and other items needed to support development or modification of applications when contractor's assistance is needed.
- Pay monthly billings in a timely manner.
- Timely notification to MNIT of errors or discrepancies in billings.
- Message/prompt changes will be supplied to MNIT, to the agreed upon MNIT staff. In an emergency, CUSTOMER'S direction to MNIT will include the emergency status as well as the message/prompt change.
- CUSTOMER will request, in writing, the changes to the CCM environment allowing MNIT a minimum turnaround of three business days. In an emergency, customer will clearly lay out any emergency need for quicker service.
- CUSTOMER will request, in writing, configuration of telephone numbers to be used with its applications allowing MNIT a minimum turnaround of three business days. In an emergency, CUSTOMER will clearly lay out any emergency need for quicker service.

## When will regular maintenance be performed?

---

To ensure optimal performance of MNIT Voice services, routine maintenance will be performed on a regular basis. The service unavailability during scheduled maintenance windows will be excluded from the uptime calculations. The maintenance is performed during the time specified in the sections below.

MNIT will provide customers a 5-business day advance notice of scheduled maintenance. All prescheduled systems maintenance, unless otherwise agreed upon in advance by Service Operations, shall be performed on the following schedule:

Description	Schedule
Classic Voice services	As required, coordinated with external vendors and communicated to customers
MNIT-provisioned services	Weekdays 4 a.m. to 6 a.m. CDT, or weekends
MNIT-provisioned services: monthly security patches	As required

## Change Management Process/Termination

---

Minnesota IT Services follows established enterprise change management procedures and processes.

## Service Name: Wide Area Network (WAN) Services

Revision Date 09/01/2021

## Executive Summary

---

Service Details	Summary Description
Service Name	<a href="#">WAN</a>
Included	<ul style="list-style-type: none"> <li>IP Network Connection</li> </ul>
NOT included	<ul style="list-style-type: none"> <li>Applications running on the MNET network</li> </ul>
Delivery Method	<ul style="list-style-type: none"> <li>Managed circuits and WAN devices</li> </ul>
Hours of Operation	<ul style="list-style-type: none"> <li>24 x 7 x 365</li> </ul>

## Description

---

MNIT WAN services provides secure network connections to state locations. These connections provide access to applications and information that employees need to do their work. WAN services connect agency sites to the state network known as Minnesota's Network for Enterprise Telecommunications (MNET), to the internet and to MNIT Enterprise Data Centers.

## What systems or services are supported?

---

WAN services provide various levels, or tiers, of network capacity and availability to align with business needs. Each tier provides a specified amount of network capacity (bandwidth) geared to support the peak levels of business activity at a location.

The employee counts shown below are approximate, as the preferred capacity at a location may depend upon additional factors. Some telecommunication circuits are not available in certain areas of the state, so all WAN tiers are not available at all locations.

The top tiers generally use dedicated circuits. The others use internet connections, but with secure and encrypted connections that are made to the MNET using a technology known as hardware-based virtual private network (VPN).

## What services are included?

---

The following levels of service are provided:

- Headquarters: Generally, for offices 501+ employees
- Branch office: Offices with 101 to 500 employees
- District office: 26-100 employees
- Field office: 13-25 employees
- Small office: 2-12 employees using a commercial internet connection
- One Person office: One person or no staff for on-net monitoring functions using an internet connection.

## What services are NOT included?

---

- One-time and recurring charges for circuits.
- WAN architecture and detailed design work is billed separately on a per hour basis.
- End user connections provided by LAN service connections will be made in coordination with the LAN team.

## How will the service be delivered?

---

Each MNIT Services customer has a designated Enterprise Relationship Manager who works with the customer on an individual basis for their IT service needs. In partnership with the Installation Coordinators and Service Managers, the Relationship Manager:

- Facilitates service implementation.
- Coordinates MNIT Enterprise Services staff and resources as needed.
- Provides consultation, needs assessment, analysis, and cost-effective solutions.
- Develops proposals and service agreements.
- Assists with writing procurement specifications.



## What are the hours of operation and how to get support?

---

### MNIT Service Desk Contacts

<b>Business Hours:</b>	24 x 7
<b>Contact Name:</b>	MNIT Enterprise Service Desk
<b>Phone Number:</b>	651-297-1111
<b>Website and Service Catalog:</b>	<a href="http://mn.gov/mnit">mn.gov/mnit</a>

## What will the response time be?

---

Response Level	Definition	Example	Response Target	Return to Service Target
Priority 1 Critical	Any Incident that has “massive impact” and is highly visible, impacts a significant number of users, a major agency, application or service, and has no redundancy or alternate path.	A State correctional facility, agency HQ, county gov’t., or HE Campus is offline	15 minutes	2 hours  Subject to vendor commitment
Priority 2 High	Incident deemed to have a high impact by being highly visible, impacting a significant number of users, impacting a major agency, application or service, where there is no redundancy or alternate path, and a bypass is unavailable	A regional or field office is offline, or the connections are running in a diminished capacity	2 hours	8 hours  Subject to vendor commitment
Priority 3 Med	Incident deemed to have a medium impact by being visible, impacting a limited number of users, where a resource or service is down or degraded.	A small office is having intermittent connections over their ISP connection	8 hours	2 business day  Subject to vendor commitment
Priority 4 Low	Any incident that impacts a small number of users or a single user where a resource or non-critical service is down or degraded and a deferred fix or maintenance is acceptable.	A one-person office has intermittent connections over their ISP connection	4 hours	5 business days  Subject to vendor commitment

## What are the business responsibilities?

---

- Identify organizational strategy and new business initiatives which may affect WAN capacity or features.

- Identify locations needing WAN connections, capacity requirements per location and hours of operation per location.
- Provide any outage blackout windows that should be avoided.
- Provide secured space at each location for WAN devices and circuit termination.
- Provide location contact information (names, phone numbers, email addresses).
- Submit service requests for adding, changing or removing WAN connections.
- Agree to contract term agreements for leased line access facilities.
- Notify the MNIT Service Desk of issues or incidents.

## When will regular maintenance be performed?

---

To ensure optimal performance of WAN services, routine maintenance will be performed on a regular basis by MNIT Services and their external partners. The service unavailability during scheduled maintenance windows will be excluded from the uptime calculations.

MNIT Services will provide customers a 5-business day advance notice of scheduled maintenance. All prescheduled systems maintenance, unless otherwise agreed upon in advance by Service Operations, shall be performed on the following schedule:

Description	Schedule
Major changes	Saturdays - 4 p.m. to 12 a.m. CDT
Carrier requested changes	Any day of the week 10 p.m. to 6 a.m. CDT
Minor planned changes	Weekdays 4 a.m. to 6 a.m., or weekends CDT

## Change Management Process/Termination

---

MNIT follows established enterprise change management procedures and processes

# Mobile Device Management/MNIT Enterprise Services

Revision Date 09/30/2021

## Executive Summary

Service Details	Summary Description
Service Name	Mobile Device Management (MDM)
Included	<ul style="list-style-type: none"> <li>• Assist customers with final device setup</li> <li>• Refresh devices on a regular replacement cycle</li> <li>• Securely dispose of devices that reach the end of their useful life</li> <li>• Device enrollment through the Enterprise Service Desk</li> <li>• Security standards, feature restrictions and application testing established by Enterprise Security Office</li> <li>• Monitor devices for compliance with security policies and operating system requirements</li> <li>• Management of data on lost devices (may include remote wipe)</li> <li>• Establish retirement parameters and replacement of non-compliant mobile device hardware</li> <li>• Facilitate delivery of agency approved applications</li> <li>• Maintain troubleshooting knowledgebase and remote diagnostics</li> </ul>
NOT included	<ul style="list-style-type: none"> <li>• All accessories other than case and screen protector</li> </ul>
Delivery Method	<ul style="list-style-type: none"> <li>• Fulltime staff for both remote and deskside support</li> </ul>
Hours of Operation	<ul style="list-style-type: none"> <li>• 24x7x365 with following hours of support:</li> <li>• M-F; 7 a.m.-5 p.m.</li> </ul>

## Description

---

This service secures and manages mobile devices that connect to the state network. The service is available for both State-owned and personally owned devices (also referred to as “bring your own device” (BYOD)).

MDM provides advanced services for mobile phones and tablets as outlined below (Windows-based tablets are covered under the Desktop-Laptop Bundle). MDM enforces role-based standards established by the Enterprise Security Office (ESO). More restrictive policies, meeting specific business requirements, can be applied with ESO review and approval.

- **Standard MDM Services**
  - **Standard MDM Services are required for all state-owned devices**
  - Offers the following features (limitations may exist depending on device type):
    - Basic capability to connect to email and calendars if required
    - Device tracking for compliance to meet hardware and software policy requirements
    - Remote device enrollment including set up and rule creation
    - Agency partners can set secure use features such as passcode and encryption requirements, compliance rules for usage, activities that are allowed on the device, and adding and controlling specific applications for business needs
    - Options for sending updates to the device, including remote wipes, if necessary. Wipes can be limited to organizational data, leaving personal files intact.
  - Support can be provided by using remote diagnostics (Bomgar/Beyond Trust).
  - **As allowed by respective agencies** - services are also available to state employees who bring their own device to work (BYOD) and utilize Mobile Application Management (MAM) without MDM. MAM is non-billable.
    - Provides basic capability to connect to email and calendar
    - Reports on active MAM connections
  - Workstation support, including remote desktop and deskside support

## Service Delivery Method

---

The service can be obtained by submitting a ticket via the Minnesota Service Hub.

- The Mobile Device Management Bundle is monthly recurring charge.
- Per state policy as issued by MMB all state-owned devices must be covered by the MNIT provided MDM advanced service
- Devices covered by MDM

- Standard mobile phones: iOS (iPhone) and Android
- Standard iOS (iPad) and Android tablets
- Mobile Hotspots

## What are the hours of operation and how to get support?

- 7x24x365 up time with following support hours - M-F, 7 a.m.-5 p.m.
- Submit requests through the Minnesota Service Hub – MDM Support
- Submit break/fix incidents through the MNIT Service Desk

## What will the response time be?

Response Level	Definition	Example	Response Target	Return to Service Target
Priority 1 Critical	Interruption making a critical functionality inaccessible or a complete interruption causing a severe impact on public-facing services availability.	All users at an agency are unable to log into the network causing an impact to public services.	30 minutes	*Immediately
Priority 2 High	Critical functionality or accessibility interrupted, degraded or unusable, having a severe impact on internal services availability. No acceptable alternative is possible.	Users are unable to access a critical application; the impact is limited an individual agency.	1 hour	12 hours
Priority 3 Medium	Non-critical function or procedure, unusable or hard to use having an operational impact, but with no direct impact on services availability. A workaround is available.	Email encryption is intermittently failing	24 hours	72 hours
Priority 4 Low	Application, procedure, or peripheral device is unusable for an individual user.	A user's docking station or external monitor is not functioning.	48 hours	120 hours

\*Note: Priority 1 service interruptions receive the highest priority and focus until the issue is resolved. The goal is to restore functionality as soon as possible.

## **What are the business responsibilities?**

---

- Onboarding/off-boarding through Minnesota Service Hub
- Submit Minnesota Service Hub tickets for moves, adds, changes and incident support
- Provide information support to assist with incidents and work orders

## **When will regular maintenance be performed?**

---

- As updates and patches are provided from the equipment manufacturer or software provider

## **Lost, stolen or damaged equipment caused by negligence**

---

This is the responsibility of the agency.

## **Change Management Process/Termination**

---

Minnesota IT Services follows established enterprise change management procedures and processes.

# Service Name: Salesforce Development & Support (SFDC) – Center of Excellence

Revision Date 08/27/2018

## Executive Summary

Service Details	Summary Description
Service Name	<a href="#">Salesforce Development and Support (SFDC) – Center of Excellence</a>
Included	<ul style="list-style-type: none"> <li>Development services, licensing, storage, platform support, add-on software, professional services.</li> </ul>
NOT included	<ul style="list-style-type: none"> <li>Direct end user support of delivered solutions. Customers must respond to end users and escalate support requests to the MNIT when necessary.</li> </ul>
Delivery Method	<ul style="list-style-type: none"> <li>Service agreements define project scope, deliverables, and development resources. Professional services hours are billed for development and support.</li> </ul>
Hours of Operation	<ul style="list-style-type: none"> <li>Production availability 7x24x365</li> </ul>

## Description

Salesforce Development and Support helps business partners create and manage custom solutions on the Salesforce platform. The group provides licensing, storage, hosting, and professional services.

## What systems or services are supported?

SalesForce is a Software as a Service (SaaS) cloud-based provider. MNIT Services Salesforce Development and Support (SFDC) – Center of Excellence (COE) authored solutions are deployed into the vendor cloud. SFDC – COE solutions are frequently used to support agency professional and occupational licensing, customer relationship management, and enforcement and inspections business processes.

## What services are included?

- Licensing: The user licensing costs incurred by Software Application Development and Support (SADS) projects are charged back to the business partner.



- **Storage:** When standard storage limits/capacities are exceeded, the team can provide additional storage.
- **Platform Support:** Provides the required application hosting infrastructure.
- **Add-on:** For non-standard product licensing, a service code is available to accommodate unique features only needed by certain clients.
- **Professional Services (Basic, Intermediate, and Advanced):** MNIT staff and/or contractors develop, implement, maintain, and/or support projects and applications. Basic, Intermediate or Advanced Professional Service codes may be used to recover costs.

## What services are NOT included?

---

- Custom developed applications are unique implementations of customer requirements. As such, the service does not include direct end user support of the delivered solutions. Each customer will work with the development team to define their requirements and include plans for how the custom application will be supported. In most cases, the customer's own staff will respond to end user support requests and then escalate issues to the development team as necessary.
- Supplemental programming such as Java or ASP.net will be provided by the customer. The Salesforce team does not provide non-Salesforce programming services.

## How will the service be delivered?

---

Applications developed with Salesforce will be delivered through the Salesforce government cloud infrastructure.

## What are the hours of operation and how to get support?

---

- Production availability 7x24x365.
- Service hours for Salesforce Development and Support:
  - Support staff on premise 8 a.m.-5 p.m. Monday-Friday (except holidays).
  - On-call support is not available.
- Submit requests and break/fix incidents through the MNIT Mall - Service Catalog or MNIT Service Desk– 651-297-1111 or toll-free 888-717-6688.

## What will the response time be?

Response Level	Definition	Example	Response Target	Return to Service Target
Priority 1 Critical	<p>The service is not operational for multiple users during scheduled availability.</p> <p>A major function of the service is not operational for multiple users during the hours that the service is scheduled for availability.</p> <p>Security Services has identified a breach of a critical system.</p>	<p>Customers cannot reach a cloud-based Salesforce URL</p> <p>Services are unresponsive</p>	15 minutes	2 hours
Priority 2 High	<p>A minor function of service is not operational for one or more users (who can continue to use other service functions).</p> <p>A customer needs administrative assistance.</p>	<p>Email messages generated by an application are being queued and delayed.</p> <p>A new application administrator needs access to the service.</p>	2 hours	8 hours
Priority 3 Med	<p>A major function of the service is reported as non-operational during non-business hours.</p> <p>A customer has questions about the service functionality or needs assistance in using the service.</p> <p>Enhancement requests.</p>	<p>Warning message edit request.</p> <p>Change to max allowed file upload size.</p>	8 hours	2 days
Priority 4 Low	<p>The service is not operational for one or more users outside of normal business hours of availability.</p>	<p>User reports connectivity problem not affecting other users.</p>	5 business days	10 business days

## What are the business responsibilities?

---

- The business must plan for application development time. Services are subject to staff availability. If necessary, staff support is not available in a timely manner, MNIT may work with business partners to find vendors capable of following team development guidelines.
- The business must recognize that Salesforce is a large product with many capabilities. MNIT attempts to define the “core” and “non-core” capabilities of these products as a reasonable boundary for determining Basic, Intermediate, and Advanced professional service levels. The boundary is not always clear and/or may change over time as software vendors frequently adjust their cloud product features and capabilities.
- When business partners make use of non-core capabilities it will be difficult for MNIT staff to assist with support issues. For this reason, MNIT staff will expect business partners to maintain and share design, management, and governance documentation related to use of the capability.
- As vendor features change, there may be upgrades and changes that necessitate rework and/or changes to the professional services work product provided by MNIT. This work may require additional payments.

## When will regular maintenance be performed?

---

- Salesforce is a subscription service delivered by the vendor through a cloud infrastructure. Overall service up time is 99.9%.
- For required maintenance, services are occasionally unavailable or read-only for short periods of time during non-business hours. Customers will be notified of downtime in advance if longer than a few minutes during business hours.

## Change Management Process/Termination

---

- MNIT uses an Agile application development process to develop custom solutions. All application development work is project-based, with associated management, documentation, and professional services requirements.
- Customers can work with MNIT to define specific change management and service termination requirements as part of the agreed upon professional services.

# Local Services Summary

Revision Date 01/12/2022

## Description

---

Local Services are provided through a wide variety of Applications utilized across administration areas throughout the Minnesota Department of Human Services (DHS) and MNsure. Applications supported by MNIT and serving both DHS and MNsure are listed in the DHS/MNsure Application Inventory System (AIS), which is administered by MNIT. The AIS serves as the system of record for applications utilized by both agencies. Information contained in the AIS includes the following:

- Application name and description
- Services and systems supported, including any dependents and interfacing applications
- Available support days and hours
- Recovery Time Objective (RTO) and Recovery Point Objective (RPO)
- Business and technical contacts, and a variety of other Security and technical information.

The AIS is designed to provide a portfolio of applications that is regularly updated to reflect new and retiring applications as well as changes to current applications in the portfolio. Reports can be retrieved from the AIS by MNIT, DHS and MNsure staff. Each listing in the AIS includes the Business Division Director, Business Manager, Primary Technical Manager, Technical Contact, and a DHS/MNsure Recovery Director.

The AIS Administrator is a MNIT DHS role that works to ensure data within AIS is current and coordinates with the application contacts, and the DHS Business Continuity Director to ensure data in AIS is current. Changes, including enhancements, to the AIS application are managed by the AIS Administrator. While changes to application data are primarily the responsibility of individual application contacts the AIS Administrator may make updates at times at the direction of application stewards. Access to the AIS is role based and audited on a quarterly basis by the AIS Administrator.

The URL to access AIS production is: <https://tnt20.agileapps.dhs.state.mn.us/agileapps/>

## What systems or services are supported?

---

- All Applications identified in AIS

## What services are included?

---

- Budget Support

- DHS works closely with MNIT staff partnering with DHS on budget and fiscal matters. The [Financial Architecture Domain Team](#) (FADT) is a governance group of DHS and MNIT representatives that meets regularly. The following exhibits reflect this business relationship and the intended outcomes:
  - [FY 2022 Financial Status Report](#)
  - [Budget Components](#)
- Functional support
  - The [IT Program Structure Roles and Responsibilities](#) document describes the functional roles and responsibilities of MNIT staff for project-based IT work. MNIT acts as a partner to the business and facilitates execution of projects. These include:
    - Program and Project Management
    - Business Analysis (BA)
    - Technical Development
    - Quality Assurance (QA)
    - Release Management
    - Communication and Reporting
    - Financial and Budget Management
    - Contract Management

Some DHS and MNSure functions are supported by combinations of Enterprise and Local Services.

- Oversight and governance of DHS IT programs consist of the following governance organizations:
  - Enterprise Architecture Board ([EAB](#)), which includes cross agency representation
  - Integrated Human Services Executive Steering Committee ([I-ESC](#)), which includes cross agency representation
  - Program Management Team ([PMT](#)), which includes cross agency representation
  - Systems Governance Groups ([SGG's](#))

The [Governance Structure Diagram](#) describes the structure of the above governance organizations. Governance Structure are always evolving and therefore the diagram may be updated from time to time. describes the structure of the above governance organizations.

## **What services are NOT included?**

---

- Any services that are not explicitly included in the “What services are included?” section above.

## **How will the service be delivered?**

---

- Service delivery is recorded in AIS for each application, or in the SLA for services that are not provided through an application.

## **What are the hours of operation and how to get support?**

---

As Partners in Performance, MNIT strives to provide the highest levels of service to agency partners. Support services can vary by application based on several factors. The following points reflect how support is delivered.

- Hours of Operations, Method of support, and support contacts can be viewed per application in AIS. If nothing is specified in AIS, it is assumed to be Monday – Friday, 7 AM – 5 PM Central Time.
- Service requests are submitted by contacting the MNIT Service Desk at 651-297-1111

## What will the response time be?

Response Level	Definition	Example	Response Target	Return to Service Target
Priority 1 Critical	<p>The service is not operational for multiple users during scheduled availability.</p> <p>A major function of the service is not operational for multiple users during the hours that the service is scheduled for availability.</p> <p>A breach of a critical system has occurred.</p>	<p>Server-related Software / Hardware issues</p> <p>Ransomware</p> <p>Distributed Denial-of Service</p>	15 minutes	2 hours
Priority 2 High	<p>A minor function of service is not operational for one or more users (who can continue to use other service functions).</p> <p>A customer needs administrative assistance.</p>	<p>Individual account lockouts</p> <p>Desktop/laptop failure</p>	2 hours	8 hours
Priority 3 Med	<p>A major function of the service is reported as non-operational during non-business hours.</p> <p>A customer has questions about the service functionality or needs assistance in using the service.</p>	<p>After-hours account lock outs</p> <p>After-hours desktop/laptop failure</p>	8 hours	2 days
Priority 4 Low	The service is not operational for one or more users outside of normal business hours of availability.	License is expiring soon.	5 business days	10 business days

## What are the business responsibilities?

- The business must plan for application development time and maintenance windows. Services are subject to staff availability. In the event staff support is not available in a timely manner MNIT may work with business partners to find vendors capable of following team development guidelines.
- Business users are responsible for reporting service issues and security issues, including potential security issues, promptly to the MNIT Service Desk at 651-297-1111.

## **When will regular maintenance be performed?**

---

- Maintenance hours are listed per application basis in AIS.
- As updates and patches are provided from the equipment manufacturer, they will be prioritized and scheduled for implementation.
- Any updates are planned, scheduled, and performed within the existing change management windows.

## **Change Management Process/Termination**

---

- Minnesota IT Services follows established enterprise change management procedures and processes.



# Service Name: Mainframe

## Executive Summary

Service Details	Summary Description
Service Name	<a href="#">Mainframe Service</a>
Included	<ul style="list-style-type: none"> <li>Batch, Workload Scheduling, Mainframe Processing, Databases on the Mainframe, Mainframe DR services, replicated storage</li> </ul>
NOT included	<ul style="list-style-type: none"> <li>Other Hosting services like Server and Hosting, Databases like SQL and Oracle, customer application support</li> </ul>
Delivery Method	<ul style="list-style-type: none"> <li>Fulltime support staff and provided mainframe equipment and infrastructure</li> </ul>
Hours of Operation	<ul style="list-style-type: none"> <li>M-F; 6 a.m.-6 p.m. on premise staff support, on-call during off hours and weekends</li> <li>24x7x365 expected infrastructure up time</li> <li>24x7x365 on site Batch Scheduling and Operations.</li> </ul>

## Description

Mainframe Services consist of many components that comprise a highly available and secure environment to house agency applications and systems. The specific quantity and location of any component will be decided by the requirements of each application and system. Ongoing management and analysis will ensure that components are configured to run in a highly secure fashion at a high level of efficiency.

## What systems or services are supported?

- Compute
- Storage
- Batch Scheduling
- Data center network
- Space and utilities
- Security
- Software licensing and management tools

## What services are included?

---

- Customer Information Control System (CICS)
- CPU, System z Integrated Information Processor (zIIP)
- Reads (e-reports)
- Scheduled jobs / job monitoring
- Data storage in gigabytes (GB)
- Backups in gigabytes (GB)
- Mainframe Database (DB2 and Adabas)
- Mainframe data replication
- Mainframe DR services

## What services are NOT included?

---

- WAN connectivity (covered in related section)
- Distributed Server Hosting (covered in related section)
- Management and use of the business side application (covered in related section)
- Use and support of databases (covered in related section)

## How will the service be delivered?

---

Fulltime support staff and provided mainframe equipment and infrastructure

## What are the hours of operation and how to get support?

---

- 24x7x365 expected infrastructure up time
- M-F, 6 a.m.-6 p.m. on premise staff support
- On-call off hours and all-day Saturday and Sunday
- 24x7x365 batch monitoring
- Submit requests through the MNIT Mall - Service Catalog
- Submit break/fix incidents through the MNIT Service Desk

## What will the response time be?

---

Response Level	Definition	Example	Response Target	Return to Service Target
Priority 1 Critical	Mainframe not available to a significant number of users.	Mainframe or LPAR not responding.	15 Minutes	2 Hours
Priority 2 High	Slow response affecting agency application for a significant number of users.  Important changes for nightly batch.  Minor function is not operational for many users (who can continue to use other application functions)	Transactions looping or run-away process. Excessive workload exceeding capacity.	2 hours	8 hours
Priority 3 Med	Minor function of the service is not operational for a few users. (who can continue to use other application functions)	Individual user cannot access the mainframe due to interface issue.	8 hours	2 business days
Priority 4 Low	A non-critical function is not available to support staff. Usually not a public facing function.	License is expiring soon.	2 business days	5 business days

## What are the business responsibilities?

---

- Assist in creating realistic expectations
- Initiate new requests
- Submit requests for changes to mainframe environment or batch schedules
- Submit request to decommission mainframe resources or batch schedules
- Report any issues as soon as possible through MN.IT's enterprise service desk
- Work with MNIT to schedule periodic IPL's needed for maintenance

- Participate in Disaster Recovery exercises

## **When will regular maintenance be performed?**

---

- As updates and patches are provided from the equipment manufacturer, they will be prioritized and scheduled for application.
- Any updates are planned, scheduled, and performed within the existing change management windows.

## **Change Management Process/Termination**

---

Minnesota IT Services follows established enterprise change management procedures and processes.

## Section 3: Service Agreement – Performance Metrics

*Revision 10/28/2021*

This section provides links to information related to the various performance metrics provided to agencies. Further information regarding each metric is available through the agency based CBTO or their designee.

### Performance Metrics

---

#### 1. Security Performance Reports/Metrics:

- a. Vulnerability Tracking Report - available to CBTOs and targeted teams (contains sensitive info on vulnerability compliance)
- b. Security Operations Center Incident Report - provided monthly to CBTOs, LOB Managers, and Agency Commissioner/leadership
- c. Semi-Annual Security Scorecard – provided to agency CBTO (and business leaders depending on agency involvement)
- d. Daily Security Briefing – Held live to update MNIT Security Line of Business Managers and partner teams on the current cyber threat landscape, recent cybersecurity events, and metrics tracked by other enterprise security teams related to vulnerability management, enterprise policies/standards, and identity and access management operations

MNIT Security Line of Business Managers for each agency can provide detail pertaining to the reports listed above.

#### 2. Enterprise Services Incident and Response Metrics:

The [Incident and Response MTTR Dashboard](#) Mean Time to Resolve report provides metrics related to MNIT service performance that can be sorted and viewed by service, agency, CBTO, as well as priority and resolve date.

CBTOs may provide other metrics, including those representing locally delivered services as needed.



---

***Open Enrollment Support  
Agreement between MNsure  
and MNIT Partnering with the  
Department of Human  
Services and MNsure***

2022 OPEN ENROLLMENT

11/01/2021 – 01/15/2022

---

## Scope and Purpose

The FY 2022 MNsure Open Enrollment period begins at 8:00 AM on Monday, November 1, 2021 and runs through Saturday, January 15, 2022 (12:00 AM on Sunday, January 16, 2022).

This document identifies hours of support for the MNIT@DHS/MNsurre support teams, the contact information for staff at both MNIT@DHS/MNsurre and MNsure, and the processing steps and expected service level goals for responses to incidents reported by MNsure during Open Enrollment.

Revision History

Description	Date of Change	Revision number
Initial version copied from 2021 OE Documents	09/08/2021	V1.0
Updated with MNsure OE dates (11/1/21-1/17/22)	09/14/2021	V2.0
Minor changes and clarifications		
Minor changes and clarifications	09/24/2021	V3.0



## MNIT Support Hours

### MNIT@DHS/MNsure Service Desk (Tier 2) Core Hours

---

Core hours for MNIT@DHS/MNsure Service Desk (Tier 2) are:  
Monday – Friday 7 a.m. – 5 p.m.

### Tier 2 Core Hours during Open Enrollment

---

Core hours for Tier 2 during Open Enrollment are 1 hour prior to the MNsure Call Center opening until the MNsure Call Center Phone queue is clear. Please refer to the [MNsure OE9 Hours of Operation](#) document for scheduled times.

### MNIT Support Outside of Core Hours

---

MASBlue will provide support outside of Tier 2 core hours.

### Changes to Support Hours during Open Enrollment

---

MNsure will notify Tier 2 of any changes to Call Center schedules that would require changes to the Tier 2 Core Hours during Open Enrollment.

MNIT will notify the MNsure Operations Group of any scheduled maintenance, planned outages or changes to work schedules that would impact system availability.

### MNIT Enterprise Service Desk (ESD)

---

The MNIT ESD is available 24 hours a day, 7 days a week for infrastructure, telecom, network and security incident support.

## MNIT and MNsure Contact Information

### MNIT Contact Information

---

*MNIT@DHS/MNsure Service Desk (Tier 2)*

**Website:** [EDI TIER 2 Issue Reporting - MNsure](#)

MNsure will use this website to report new incidents to Tier 2. When an incident is entered, it is stored in the ticketing software used by Tier 2 for tracking. All METS Tier 2 staff are notified of all tickets when they are logged.

**Email:** [metstii@state.mn.us](mailto:metstii@state.mn.us)

MNsure will use this address to reply to questions or requests for status updates on incidents, or when providing additional information as requested by Tier 2.

MNIT will use this address to provide incident updates and request additional information from MNsure.

#### *Tier 2 Escalations*

MNsure will escalate incidents or requests prioritized Critical or High when updates are not provided by MNIT or that need immediate attention.

**Kent Smith (MNIT@DHS/MNsure Service Desk Supervisor)**

Email: [kent.smith@state.mn.us](mailto:kent.smith@state.mn.us)

Phone: 651-431-6307 (work)

651-363-1275 (mobile)

**Debra Tibstra (Application Services Director)**

Email: [deb.tibstra@state.mn.us](mailto:deb.tibstra@state.mn.us)

Phone: 651-431-4074 (work)

651-755-7326 (mobile)

#### *Tier 2 Contact Outside of Core Hours*

Major Application Support Blue team (MASBlue)

**Email:** [#DHS MN.IT MAS Blue](#)

MNsure will use this address to report Urgent and Critical incidents outside of Tier 2 Core Hours

*Tier 3 Support Teams Contact Information*

Tier 2 will email the following teams when they need to escalate to the technical support teams

**MN\_DHS\_DHS Tier2**

**#MNEIAM\_IAM\_TEAM**

**#DHS\_MN.IT@DHS-OAM\_Team**

**#DHS\_TPIN**

**#DHS\_MN.IT\_MAS\_Blue**

---

## MNIT Enterprise Service Desk

---

*Infrastructure, Network, Telecom, Security Incidents*

**Website:** [Minnesota Service Hub](#)

**Phone:** 651.297.1111

*For Critical Incidents, please call the ESD and select option 9 – Critical Outage instead of using the website.*

## MNsure Contact Information

---

### *MNsure Operations Group*

**Email:** [#Mnsure Mnsure Operations and Issues Group](#)

MNIT will use this address when acknowledging Incident/Request submission, providing updates or when requesting additional information from MNsure. MNIT will also use this address to notify MNsure of any scheduled maintenance, planned outages or changes to work schedules that may impact system availability or the MNsure Contact Center hours.

### *MNsure Leadership Contact Information*

**Email:** [#Mnsure Mnsure Business Operations Leadership](#)

MNIT will use this address to notify or acknowledge Critical incidents that are identified, reported or resolved.

### *MNsure Escalation Information*

MNIT will escalate for Critical or High priority incidents when timely responses are not provided by MNsure or that need immediate attention.

#### **Jolene Wright (MNsure Program Operations Director)**

Email: [jolene.l.wright@state.mn.us](mailto:jolene.l.wright@state.mn.us);

Phone: 651-238-3743

# Incident Management Processes

## Incident Reporting

---

MNsure will record incidents in the [Business & Ops Issues \(BOPS\) Log](#) on the MNsure internal SharePoint site.

MNsure will provide update access to the BOPS list to MNIT Tier 2 staff so updates can be applied as needed.

MNsure will submit all incidents and requests using the EDI Tier 2 Issue Reporting – MNsure website (see link in Contacts section above). For Critical and Urgent incidents, MNsure may *also* choose to send emails or call the MNIT escalation contacts listed above.

MNsure will use the **Urgency** field on the web form to identify the incident's priority. At this time, the *Urgency* field does not provide a 'Critical' value so if MNsure determines the incident priority is Critical, MNsure will use the 'High' urgency value and place the word 'Critical' at the beginning of the Problem Description field.

For incidents sent via email to Tier 2, MNsure will identify the Priority of the incident in the Subject line.

## Incident Response

---

MNIT @ DHS/MNsure staff will log tickets with the Enterprise Service Desk using Minnesota Service Hub (link in Contacts section) website or via phone.

When an Incident is received by Tier 2 they will:

Email the **MNsure Operations and Issues Group** to acknowledge receipt of the incident and, if necessary, request additional information.

Perform initial triage of the incident to determine:

- Is this a known defect?
- Is there a work around available?
- Is this an incident that can be resolved by Tier 2?

Based on Initial triage results Tier 2 will:

- Perform resolution steps
- Email **MNsure Operations and Issues Group** with resolution information
- Update BOPS log with resolution

-- Or --

- Provide Work Around solution to MNSure
- Verify the work around will resolve the incident
- Or --
- Contact Tier 3 technical support teams (See contact information) with incident detail and triage results
- Log an incident with the Enterprise Service Desk when needed
- Record the ESD Request number in Tier 2 ticket and in BOPS log

The following table outlines the incident priority definitions and Service Level Goals for each.

Priority	Definition	Service Level Goals
Critical  <i>(MNSure will record the urgency as "High" on the Tier 2 Reporting Form since "Critical" is not available in the drop list)</i>	An outage of MNSure enterprise-wide services that affects all users at a main campus, is likely to cause significant financial loss or critical data loss, or seriously impairs regular ongoing work of MNSure as it relates to customers and partners.	<ul style="list-style-type: none"> <li>• Notification or acknowledgment to <b>MNSure Ops Leadership</b> contact within 20 minutes of a Critical incident being identified or reported</li> <li>• Incident resolution within 2 hours and confirmation to <b>MNSure Ops Leadership</b> contact</li> <li>• Conference call with <b>MNSure Ops Leadership</b> contact if issue is not resolved or will not be resolved within 2 hours</li> </ul>
High	Substantial impact on MNSure business users or customers and may cause financial or data loss, impairs non-routine work of MNSure as it relates to its customers and businesses, and has no feasible workaround.	<ul style="list-style-type: none"> <li>• Notification or acknowledgment to <b>MNSure Ops and Issues</b> contact within 2 hours of a High issue being identified or reported</li> <li>• Incident analysis and assessment, and update to MNSure within 8 hours</li> </ul>
Medium	Limited or confinable impact on business users or customers, minimal work impairment and a reasonable workaround is available.	<ul style="list-style-type: none"> <li>• Notification or acknowledgment to <b>MNSure Ops and Issues</b> contact within 8 hours of a Medium issue being identified or reported</li> <li>• Issue analysis and assessment, and update to <b>MNSure Ops and Issues</b> within 2 business days</li> </ul>

Low	Insignificant impact on business users or customers, and a known reliable workaround is available.	<ul style="list-style-type: none"><li>• Notification or acknowledgment to <b>MNsure Ops and Issues</b> contact within 8 hours of a Low issue being identified or reported</li><li>• Issue analysis and assessment, and update to <b>MNsure Ops and Issues</b> within 5 business days</li></ul>
-----	--	--

## Incident Investigation and Mitigation

When Tier 2 is unable to resolve an incident, they will email the Tier 3 Support teams (See Contact section) with the incident information and all actions taken up to that point.

The OAM Business Analysis team will log the incident in their operations log for tracking. Any CCM (Change and Configuration Management) tasks needed for technical support will be created by the OAM BA teams.

If a MNIT Enterprise Support team is required (i.e. MNEIAM), Tier 2 will submit a Service Request in the Minnesota Service Hub (See Contact Information) for all Medium and Low Priority incidents. For Critical and High incidents, Tier 2 will call the ESD phone number to log the ticket with the appropriate priority.

Tier 2 will be the primary contact between Tier 3 and MNsure for all incident communications. This includes requests for information/conference calls, testing needs, resolution and post resolution follow-up.

If the Technical support teams need direct communication with MNsure via conference call, Webex or Teams meetings, these should be requested via Tier 2.

Tier 2 will reach out to the incident reporter or to the **MNsure Operations and Issues** group to request additional information regarding incidents.

Tier 2 will document all requests for information and their responses in the CRM ticket.

MNsure will provide follow-up information and updates to the number of occurrences for a reported incident via email.

*If, during problem investigation, a **new production defect** is identified. The OAM BA team will log the defect in CCM. The defect will then follow standard OAM Defect processing steps, including defect priority determination, severity determination and resolution timelines.*

## Incident Status Reporting

---

### *Tier 2 reporting*

Obtain status updates from Tier 3 teams prior to daily MNsure Issue huddle.

Notify MNsure, Tier 3 Support Teams and/or MNIT Enterprise Service Desk of any changes in status, severity or priority for reported incidents.

Update BOPS log of any changes in status, severity or priority for reported incidents.

Actively participate in the daily MNsure Issue huddle

Assist with providing direction and oversight regarding real-time urgent incidents and requests.

Provide requests for needing information to MNsure and their response to the Tier 3 Support Team requesting the information

Notify MNsure and/or MNIT Enterprise Service Desk of system incidents or scheduled events that may impact METS performance or availability

Convey the status, severity and priority of items discussed at the BOPS daily huddle to Tier 3 Support teams and/or MNIT Enterprise Service Desk working on a reported incident.

### *Tier 3 Support Teams*

Provide status updates to Tier 2 prior to daily MNsure Issue huddle

Provide requests for needed information from MNsure to Tier 2

### *MNsure*

MNsure will notify Tier 2 of any changes in status or priority for reported incidents

Provide requested information needed on reported incidents.

For Data Warehouse reporting incidents, MNsure will follow the existing process of logging a Request with the Enterprise Service Desk. If MNsure determines that this request is Critical, they will log a Critical ticket with Tier 2 that includes the ESD Request number.



## Terms and Definitions

*Change and Configuration Management (CCM):*

The application used by MNIT@DHS/MNsure to track technical and operational activities related to METS/MNsure.

*Customer Relationship Manager (CRM):*

The application used by MNIT@DHS/MNsure Service Desk to record and track incident progress reported by MNsure and DHS.

*Defect:*

An error that causes the system to produce incorrect or unexpected results.

*Impact/Severity:*

The measure of the business criticality of an incident. Often equal to the extent to which an incident leads to distortion of, or departure from, agreed or expected service levels. Size, scale, magnitude and scope.

*Incident:*

An unplanned interruption to a service or reduction in the quality of a service.

*Incident Management:*

The practice of minimizing the negative impact of incidents by restoring normal service operation as quickly as possible.

*Known Error:*

An incident or problem for which the root cause is known and for which a temporary work around or a permanent alternative has been identified.

*Minnesota Eligibility Technology System (METS):*

Application used by MNsure and the Department of Human Services to determine applicant eligibility for public or private health care programs.

*Priority:*

The sequence in which an Incident, Problem or Change needs to be resolved, based on the impact and severity.

*Problem:*

A cause, or potential cause, of one or more incidents.

***Problem Management:***

The practice of reducing the likelihood and impact of incidents by identifying actual and potential causes of incidents, and managing workarounds and know errors.

***Work Around:***

A solution that reduces or eliminates the impact of an incident or problem for which a full resolution is not yet available. Some workarounds reduce the likelihood of incidents.



## Signature Page

Under Minnesota Statutes section 16E, Minnesota IT Services (dba MNIT) provides Information Technology services to the Agency.

The MNIT Service Level Agreement is reviewed and recognized by:

### Agency/Entity

A blue ink signature of Nathan Clark.

---

Nathan Clark  
Chief Executive Officer  
MNsure

June 23, 2022

---

Date of Signature

### MNIT Services

DocuSigned by:  
A blue ink signature of Tarek Tames.  
9BC4418FE4DE41F...  
Tarek Tames

---

State Chief Information Officer and  
MNIT Services Commissioner

7/6/2022

---

Date of Signature