MINNESOTA IT SERVICES

# Comprehensive IT FY22-23 Service Level Agreement

in direct support of

*Minnesota Department of Human Rights*

# Table of Contents

# 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 three sections:

1. Service Agreement: General Terms
2. Service Agreement: Projects and Services
3. Service Agreement: Performance Metrics

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.

# 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 (EEPMO) 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

| Service Details | Summary Description |
|---|---|
| Supporting Agency | Department of Employment and Economic Development |
| Service Name | Salesforce Development and Support (SFDC) – Center of Excellence |
| Included | • Development services, licensing, storage, platform support, add-on software, professional services. |
| NOT included | • Direct end user support of delivered solutions. Customers must respond to end users and escalate support requests to the MNIT when necessary. |
| Delivery Method | • Service agreements define project scope, deliverables, and development resources. Professional services hours are billed for development and support. |
| Hours of Operation | • Production availability 7x24x365 |

**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*

***Revision Date 10/28/2021***

# Executive Summary

| Service Details | Summary Description |
|---|---|
| Service Name | Database Administration |
| Included | • Database operational support |
| NOT included | • Database logical design<br>• Application support<br>• Dedicated host, license & maintenance costs |
| Delivery Method | • Fulltime support staff with access to MNIT on-premises and external cloud environments |
| Hours of Operation | • Production availability 7x24<br>• On-call off hours, weekends, and holidays<br>• Non-production: M-F; 7 a.m.-5 p.m. |

# Service Name: Database Support - Shared Services

## 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 | The hosted website is not operational for multiple users, or citizens during scheduled availability<br><br>A major function of the hosting service is not operational for multiple users during the hours that the service is scheduled for availability | A production site displays that an application is unavailable | 15 minutes | 2 hours |
| Priority 2 High | A user needs administrative assistance performing urgent updates or maintenance<br><br>A minor function of the hosting service is not operational for many users (who can continue to use other application functions) | Application support staff are reporting issues of concern related to aspects of production processing | 2 hours | 12 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)<br><br>A user has questions about the hosting service functionality or needs assistance in using the service | 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.

***Revision Date 07/14/2021***

# Executive Summary

| Service Details | Summary Description |
|---|---|
| Service Name | Laptop Bundle/Desktop Bundle |
| Included | • Standard Laptop, replaced every 4 years<br>• Standard Desktop, replaced every 5 years<br>• Docking station, keyboard and mouse (replaced with laptop if necessary, monitor not included)<br>• Workstation management and protection package: security patching and encryption<br>• Workstation support, including remote desktop and deskside support.<br>• Inventory management |
| NOT included | • Performance-upgraded laptop/desktop<br>• Monitor(s)<br>• Memory upgrade<br>• Headset<br>• Cameras (required to use all the functionality of Microsoft Teams)<br>• Local printer, if applicable for your agency<br>• Ergonomic or wireless bundle for keyboard and mouse<br>• Programmable keyboard<br>• Shorter refresh cycle (see details below) |
| Delivery Method | • Fulltime staff for both remote and deskside support |
| Hours of Operation | • 24x7x365 with following hours of support:<br>• M-F; 7 a.m.-5 p.m. |

# Service Name: Laptop/Desktop Bundle

## 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 deskside 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<br>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<br>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<br>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<br>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.

***Revision Date 10/18/2021***

# Executive Summary

| Service Details | Summary Description |
|---|---|
| Service Name | Enterprise Hosting Services |
| Included | • Data Center Services and Support<br>• Enterprise Cloud Services<br>• Virtual Desktop<br>• Enterprise Secure File Transfer Protocol (SFTP)<br>• Physical and virtual server management and support |
| NOT included | • Customer application support |
| Delivery Method | • Fulltime support staff<br>• Server equipment and infrastructure both on premise and in the cloud |
| Hours of Operation | • 24x7x365 expected infrastructure up time<br>• On premise support:<br>  ○ Monday through Friday, 6 a.m.-6 p.m.<br>• On call support:<br>  ○ Monday–Friday 6p.m. to 6 a.m.<br>  ○ Saturday, Sunday and Holidays |

# Service Name: Enterprise Hosting

## 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 | The hosted website is not operational for multiple users, or citizens during scheduled availability.<br><br>A major function of the hosting service is not operational for multiple users during the hours that the service is scheduled for availability. | Site displays a 404 page not found error. | 15 minutes | 2 hours |
| Priority 2 High | A user has questions about functionality or needs assistance in using the service.<br><br>A user needs administrative assistance performing urgent updates or maintenance.<br><br>A minor function of the hosting service is not operational for many users (who can continue to use other application functions). | 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.

***Revision Date 09/14/2021***

# Service Name: Enterprise Security Services

## 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 | • Internal Vulnerability Scanning of desktops, servers, network devices and other supported devices<br>• External scanning of internal facing devices<br>• Communication of prioritized vulnerabilities<br>• Oversight of remediation efforts on vulnerabilities<br>• Configuration compliance scanning (emerging capability)<br>• Web application security scanning (DAST)<br>• Veracode administration for teams using Veracode static code analysis tool (SAST)<br>  ○ Dedicated subject matter expert to assist with taking full advantage of Veracode<br>• In-depth web application security assessment (upon request)<br>• Cloud Web Application Firewall (WAF) and Bot service administration<br>• Penetration and Red Team Services (emerging capability) |
| NOT included | • Devices not connected to MNIT managed networks<br>• Devices not supported by TVMU tools |
| Delivery Method | • Fulltime support Staff<br>• Automated scanning<br>• MNIT Mall: Threat and Vulnerability Management |
| Hours of Operation | • M-F; 7 a.m.-5 p.m.<br>• Emergency after hours support: MNIT Service Desk |

# Security Operations Center (SOC)

| Service Details | Summary Description |
|---|---|
| Service Name | Security Operations Center |
| Included | • Security Incident Response<br>• SOC Daily Briefing – informed by Threat Intelligence<br>• Spam/Phishing Investigation<br>• Security Operations Coordination<br>• Security Monitoring<br>• Enterprise Intrusion Detection and Prevention<br>• Enterprise Web Content Filtering<br>• Enterprise Endpoint Protection<br>• SIEM (log collections)<br>  ○ Threat Hunting<br>• Threat Intelligence<br>• Distributed Denial of Service (DDOS) attack protection<br>• Netflow monitoring and detection for all MNet networks |
| NOT included | • Full service provided to MN executive branch and partner entities with core detection/alerting to other MNET customers<br>• Monitoring is limited to network activity only for external MNET entities that do not participate in the Intrusion Detection and Prevention Service |
| Delivery Method | • Fulltime support staff<br>• Email**:** soc@state.mn.us<br>• Phone: 651.201.1281<br>• MNIT Mall:  Report a Security Event |
| Hours of Operation | • Daily 6 a.m. – 6 p.m.<br>• Emergency after hours support: MNIT Service Desk 24x7<br>• Overwatch (365/24x7) endpoint monitoring |

# Digital Forensics

| Service Details | Summary Description |
|---|---|
| Service Name | Digital Forensics |
| Included | • Security Incident Investigations<br>  ○ Data breach incident<br>  ○ Malware/Ransomware incident<br>  ○ Intrusion incident<br>• Forensics case consultation |
| NOT included | • Devices not owned by executive branch agencies* |
| Delivery Method | • Fulltime support staff<br>• MNIT Mall: Use the Agency Data & Legal Hold Request Form<br>• Email: mnit.forensics@state.mn.us<br>• Phone: 651-201-3067 |
| Hours of Operation | • M-F: 8 a.m. to 4:30 p.m. CST<br>• Emergency after hours support: MNIT Service Desk 24x7 |

** Exceptions made upon specific incident investigation request*

# Secure Engineering and Architecture

| Service Details | Summary Description |
|---|---|
| Service Name | Secure Engineering and Architecture |
| Included | • Set the direction for Minnesota's security architecture through:<br>  ○ Development of technical security configuration and technical reference architecture standards<br>  ○ Integrating secure design principles and processes into MNIT Services projects and initiatives<br>  ○ Portfolio management and systems & applications development processes<br>• Provide Security Architect and Engineering consulting resources to enterprise projects and initiatives<br>• Operate a Payment Card Industry (PCI) program to monitor state compliance and secure Cardholder Data Environments (CDE)<br>• Provide security and compliance consulting services for agency PIC compliance<br>• Operate vender security risk management services to executive branch. |
| NOT included | LOB team security consulting |
| Delivery Method | • Fulltime support staff<br>• Email: sse@state.mn.us |
| Hours of Operation | • M-F: 8 a.m. to 4:30 p.m. CST |

# Enterprise Privileged Account Management Service

| Service Details | Summary Description |
|---|---|
| Service Name | Enterprise Privileged Account Management Service |
| Included | • User license<br>• Centralized, secure storage<br>• Automatic password rotation<br>• Automated Workflows<br>• Security Awareness training<br>• Access oversight and audit<br>• Connection manager |
| NOT included | • Storage of personal passwords |
| Delivery Method | • Fulltime Support staff<br>• MNIT Mall: Privileged Account Access |
| Hours of Operation | • M-F; 7 a.m.-5 p.m.<br>• Emergency after hours support: MNIT Service Desk |

# Enterprise Digital Certificate and Encryption Key Management (PKI)

| Service Details | Summary Description |
|---|---|
| Service Name | Enterprise Digital Certificate and Encryption Key Management (PKI) |
| Included | • Management of external digital certificates<br>• Management of internal digital certificates |
| NOT included | • Management of encryption keys |
| Delivery Method | • Fulltime Support staff<br>• MNIT Mall: Security Certificates |
| Hours of Operation | • M-F; 7 a.m.-5 p.m.<br>• Emergency after hours support: MNIT Service Desk |

## Enterprise Governance, Risk, and Compliance

| Service Details | Summary Description |
|---|---|
| Service Name | Enterprise Governance, Risk, and Compliance |
| Included | • Develop/update Minnesota's State Security Policies and Standards<br>• Maintain/manage the Archer application (RSA tool that helps us provide an integrated picture of security risk)<br>• Custodian of agency security findings and exceptions in Archer<br>• Provide support to agencies for audits/assessments that have IT security compliance requirements<br>• Conduct IT security risk assessments on applications and systems<br>• Partner with MNIT Communications to provide monthly security awareness messaging and October Cyber Security month awareness messaging<br>• Partner with vendor to ensure security awareness training is delivered to agency staff<br>• Partner with vendor to ensure that monthly phishing campaigns are sent to agency staff and that agencies receive monthly reports<br>• Security Scorecard Metrics process oversight |
| NOT included | |
| Delivery Method | • Fulltime support staff<br>  ○ Email: GRC@state.mn.us |
| Hours of Operation | • M-F, 8 a.m.-5 p.m. |

# 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.

***Revision Date 07/15/2021***

# Executive Summary

| Service Details | Summary Description |
|---|---|
| Service Name | Enterprise Software Bundle |
| Included | **Bundle Options:**<br>• **Standard Bundle - NEW**<br>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.<br>○ **Power BI Pro** 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.<br>○ **Audio-Conferencing Add-on** 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.<br>○ **Microsoft Cloud App Security** is included in this bundle. Agencies can determine how these enhanced security features work best with their local business processes.<br>• **Basic Bundle**<br>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. |

| | |
|---|---|
| | • **Kiosk**<br><br>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.<br><br>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.<br>• **Education Bundle**<br>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.<br>• **Exchange Online Only – NEW**<br>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. |
| NOT included | • Agency-specific software packages |
| Delivery Method | • Fulltime support staff for both online and deskside support. |
| Hours of Operation | • Access to Foundational Services (Email, SharePoint and Teams) 24x7x365 from Microsoft<br>• Following hours of Minnesota IT Services support. M-F, 7 a.m.5 p.m. |

# Service Name: Enterprise Software Bundles

## 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

- 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<br>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<br>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<br>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<br>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.

***Revision Date 09/01/2021***

# Executive Summary

| Service Details | Summary Description |
|---|---|
| Service Name | LAN |
| Included | • Wired and wireless IP network connections within a location or campus |
| NOT included | • Wide area network (WAN) connections |
| Delivery Method | • Minnesota IT Services owned and managed LAN devices |
| Hours of Operation | • 24x7x365 |

# Service Name: Local Area Network (LAN) Services

## 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

## What will the response time be?

| Response Level | Definition | Example | Response Target | Return to Service Target |
|---|---|---|---|---|
| Priority 1<br><br>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*<br><br>* Business Hours |
| Priority 2<br><br>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*<br><br>* Business Hours |
| Priority 3<br><br>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<br><br>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.

***Revision Date 09/15/2021***

# Executive Summary

| Service Details | Summary Description |
|---|---|
| Service Name | Middleware |
| Included | • Middleware software and support |
| NOT included | • Customer application support<br>• Database charges if MQ messaging is employed<br>• Dedicated host charges |
| Delivery Method | • Fulltime support staff with access to the MNIT on premise and external cloud environments |
| Hours of Operation | • Production: availability 7x24x365<br>• On-call off hours, weekends, and holidays<br>• Non-production: M-F; 7 a.m.-5 p.m. |

# Service Name: Middleware Support - Shared Services

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

***Revision Date 09/30/2021***

# Executive Summary

| Service Details | Summary Description |
|---|---|
| Service Name | Mobile Device Management (MDM) |
| Included | • Assist customers with final device setup<br>• Refresh devices on a regular replacement cycle<br>• Securely dispose of devices that reach the end of their useful life<br>• Device enrollment through the Enterprise Service Desk<br>• Security standards, feature restrictions and application testing established by Enterprise Security Office<br>• Monitor devices for compliance with security policies and operating system requirements<br>• Management of data on lost devices (may include remote wipe)<br>• Establish retirement parameters and replacement of non-compliant mobile device hardware<br>• Facilitate delivery of agency approved applications<br>• Maintain troubleshooting knowledgebase and remote diagnostics |
| NOT included | • All accessories other than case and screen protector |
| Delivery Method | • Fulltime staff for both remote and deskside support |
| Hours of Operation | • 24x7x365 with following hours of support:<br>• M-F; 7 a.m.-5 p.m. |

# Mobile Device Management/MNIT Enterprise Services

## 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<br>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<br>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<br>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<br>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.

***Revision Date 09/1/2021***

# Executive Summary

| Service Details | Summary Description |
|---|---|
| Service Name | Voice |
| Included | • Telephone service using state IP services or contracted traditional services |
| NOT included | • Cellular Phones |
| Delivery Method | • Dial tone to telephone handset and or softphone |
| Hours of Operation | • 24 x 7 x 365 |

# Service Name: Voice

## 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

## What will the response time be?

| Response Level | Definition | Example | Response Target | Return to Service Target |
|---|---|---|---|---|
| Priority 1<br><br>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<br><br>Voice Related Services – a service is non-functional for all users | 15 minutes | 2 hours |
| Priority 2<br><br>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<br><br>Voice Related Services – a service is non-functional for multiple users | 2 hours | 8 hours |
| Priority 3<br><br>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<br><br>Voice Related Services – a service for an individual user is non-functional | 8 hours | 2 business days |
| Priority 4<br><br>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.

***Revision Date 09/01/2021***

# Executive Summary

| Service Details | Summary Description |
|---|---|
| Service Name | WAN |
| Included | • IP Network Connection |
| NOT included | • Applications running on the MNET network |
| Delivery Method | • Managed circuits and WAN devices |
| Hours of Operation | • 24 x 7 x 365 |

# Service Name: Wide Area Network (WAN) Services

## 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

**Business Hours**: 24 x 7

**Contact Name**: MNIT Enterprise Service Desk

**Phone Number**: 651-297-1111
**Website and Service Catalog**: mn.gov/mnit

## What will the response time be?

| Response Level | Definition | Example | Response Target | Return to Service Target |
|---|---|---|---|---|
| Priority 1<br>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<br>Subject to vendor commitment |
| Priority 2<br>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<br>Subject to vendor commitment |
| Priority 3<br>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<br>Subject to vendor commitment |
| Priority 4<br>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<br>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

***Revision Date 09/15/2021***

# Executive Summary

| Service Details | Summary Description |
|---|---|
| Service Name | Web Management |
| Included | • Enterprise Web Content Management - SDL Web (Tridion) and Hosting<br>• Website development, design, and support |
| NOT included | • Customer application support<br>• Optional: Quality Assurance website tool and Web Analytics |
| Delivery Method | • Fulltime support staff with access to MNIT on-premise and external cloud environments |
| Hours of Operation | • Production availability 7x24x365 |

# Service Name: Web Management Services

## 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<br><br>Critical | The hosted website is not operational for multiple users, or citizens during scheduled availability<br><br>A major function of the hosting service is not operational for multiple users during the hours that the service is scheduled for availability | Site displays a 500 Internal Server Error | 15 minutes* | 2 hours* |
| Priority 2<br><br>High | A user needs administrative assistance performing urgent updates or maintenance<br><br>A minor function of the hosting service is not operational for many users (who can continue to use other application functions) | 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<br><br>Med | A user has questions about the hosting service functionality or needs assistance in using the service<br><br>A minor function of the hosting service is not operational for one or few users (who can continue to use other application functions) | 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<br><br>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

# Revision Date 02/04/2022

# Executive Summary

| Service Details | Summary Description |
|---|---|
| Service Name | Local Application Development and Maintenance |
| Included | Custom Application Development, Application Maintenance |
| NOT included | Enterprise Services, Project Management, Business Analysis, Quality Assurance, Help Desk, Communications |
| Delivery Method | State staff, consultants |
| Hours of Operation | M-F 7am-5pm, On call for some systems through batch processing |

| Service Details | Summary Description |
|---|---|
| Service Name | Local Cybersecurity |
| Included | Risk Identification, Risk Mitigation Recommendations, Risk Mitigation Implementation, Threat Infiltration Response |
| NOT included | Enterprise Services, Shared Services, Application Development, Business Analysis, Quality Assurance, Help Desk, Communications, Data Classification Definitions, Legal Advice or Consultation on Cybersecurity |
| Delivery Method | State staff, consultants |
| Hours of Operation | M-F 8am-5pm<br><br>Enterprise Security Operations Center hours 6am-6pm 7 days a week. |

# Revision Date 02/4/2022

# Service Name: Local Application Development and Maintenance

## Description

Provide local Application Development of MDHR applications. This service provides implementation of desired application features, custom programming, and application development, and on call maintenance of MDHR applications for application development.

## What systems or services are supported?

- **OnBase** Enterprise Content, Process and Case Management suite – Supported by external vendor DataBank
- Caspio
- Paystat
- OnBase ShareBase User License (DataBank)
- Zoom
- Snap Survey

## What services are included?

**Application Development**

- Design new application/functionalities upon request and approval
- Develop new application/functionalities upon request and approval
- Customization/enhancement to the existing functionalities
- Integration with third party software or programs
- Unit testing application changes
- Design and develop Batch jobs/processes
- Design and develop system or data interface files
- Manage IT Contracts

**Production Release**

- Work with business to prioritize projects/activities
- Help determine and manage release schedules

**Application Maintenance**

- Bug fixes for all existing applications
- Routine maintenance
- Production Database Change Requests
- On call support of batch jobs during the batch window
- Work with other MNIT teams and MDHR on creation and maintenance of a Disaster Recovery Plan
- Disaster Recovery supporting tasks in a disaster recovery scenario
- Reports

**Accessibility**

- Custom and customized development of user interfaces that meet the State of MN accessibility standards
- Work with vendors on meeting State of MN accessibility standards

**Cloud based Software as a Service**

- Cloud software annual support and licensing procurement
- Development and management of required data interfaces

## What services are NOT included?

- Services identified as being delivered under Enterprise Services, Shared Services or Center of Excellence Services in this document.
- Project Leadership
- First Tier End User Help Desk
- End User Training
- End User Communication
- Business Systems Analysis
- Quality Assurance Testing
- Functional Testing
- Cloud based Software as a Service solution administration

## How will the service be delivered?

- Full time staff
- Consultants
- Vendor agreements

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

Normal business day (Monday through Friday) 8:00 AM to 4:30 PM. On call support is available during system batch windows for stop call batch jobs. Support is obtained through direct contact of MNIT Management for non-emergency work or directly to the development resources for on call or emergency work.

# Service Name: Local Cyber Security

## Description

Provide local Cyber Security support of MDHR infrastructure, applications, and systems. This service utilizes the Enterprise Security Office and provides professional cybersecurity services to both MNIT and MDHR to identify potential threats, recommend solutions to minimize risk, coordinate efforts to implement approved solutions, and work with the Enterprise Security Office to coordinate actions in a cybersecurity situation and follow-up actions.

## What services are included?

**Risk identification**

- Analyze gaps in Local MDHR applications, systems, and infrastructure to Enterprise Security Standards.
- Be aware of potential risks and threat vectors and ensure MNIT management is aware of potential cyber security risks.
- Coordinate with MDHR to identify attacks through the monitoring of logging and alerts.

**Risk mitigation recommendations**

- Develop plans to mitigate potential and identified cybersecurity risks to Local MDHR applications, systems, and infrastructure.
- Present risk mitigation plans with resource requests to MNIT IT Management for approval.

**Risk mitigation implementation**

- Coordinate the execution of risk mitigation plans with MMB, MNIT, and third-party vendors as required.

**Threat infiltration response**

- Assess threat scope and signs of compromise to help mitigate attacks.
- Coordinate threat response efforts with the Enterprise Security Office, MDHR, and MNIT IT staff.
- Coordinate after action reports and actions with the Enterprise Security Office, MDHR, and MNIT IT staff.

**Security Awareness Training and Education (SATE)**

- Coordinate with MNIT Governance Risk and Compliance (GRC) to provide Annual Security Awareness Training to MMB.
- Coordinate with GRC on monthly phishing training.

## What services are NOT included?

- Services identified as being delivered under Enterprise Services, Shared Services or Center of Excellence Services in this document.
- First Tier End User Help Desk
- End User Training
- End User Communication
- Data classification definitions
- Legal advice or consultation

## How will the service be delivered?

- Full time staff
- Consultants
- Vendor agreements

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

Normal business day (Monday through Friday) 8:00 AM to 5:00 PM. Requests for work are submitted via email or phone directly to Local Cyber Security staff resources. Enterprise Security Operations Center hours 6am-6pm 7 days a week.

# For all Local Services listed above:

| Response Level | Definition | Example | Response Target | Return to Service Target |
|---|---|---|---|---|
| Priority 1<br>Critical | Major loss of production system availability or functionality resulting in direct impact to staff and their ability to perform daily work duties. This will trigger a Critical 1 if issue persists past 90 minutes. | Production system outage<br>Unplanned application outage | < 30 min | < 90 min |
| Priority 2<br>High | Significant or intermittent loss of system availability or functionality resulting in direct impact to staff's ability to perform daily work duties. Includes impact to major project work. This will trigger a Critical 1 (with or without a management bridge) if issue persists past 3 hours. | Intermittent system issues<br>application function is degraded<br>Application performance is slow | < 1 hr | < 3 hrs |
| Priority 3<br>Med | Minor loss of production system functionality with minimal impact to staff productivity or intermittent loss of system availability in non-production environments | Non-production environment intermittent issue | < 4 hrs | 2 business day |
| Priority 4<br>Low | Non-urgent system issue without impact to staff productivity | Low impact configuration issue | < 8 hrs | TBD or <2 weeks or per schedule |

Response target begins at time the issue is officially reported to MNIT. Incident Response issues are submitted through MNIT Mall ticket, or via email to MNIT Management and MNIT teams. Priority 1 or Priority 2 level requests can be submitted via direct phone call to MNIT Management.

## What services are included?

- **Responsible for incident resolution through either internal or external resources as the situation dictates.**

- **For priority 1 level incidents, communications on analysis progress and ultimate resolution will be provided to impacted MDHR business units at 30 min intervals or as otherwise agreed upon frequency.**
- **For non-priority 1 level incidents, communications on analysis progress and ultimate resolution will be provided at agreed upon intervals between MNIT and MDHR teams.**

### Request for Change

| Response Level | Definition | Example | Response Target | Move to Production Target |
|---|---|---|---|---|
| Priority 1<br>Critical | Critical system change impacting production environments and time sensitivity is required. | Production server configuration change to address cybersecurity incident | <2 hrs | ASAP dependent on the change |
| Priority 2<br>High | Significant change impacting production environments where time sensitivity is important but not a driving factor. | Addition of a new process to address system performance | <1 day | TBD dependent on the change |
| Priority 3<br>Med | Important system enhancement or change to functionality of a system required due to an executive order, legal or statutory change, or time sensitive MDHR initiative. | Implementation of a new module or functionality to comply with a change in law | <2 days | TBD |
| Priority 4<br>Low | Non-urgent system enhancement, addition of functionality, or timed event requiring specific attention or work to accomplish. | Implementation of a new module or feature | <5 days | TBD |

Response target begins at time the request for the change is officially submitted to MNIT Management as a request for work. For Request for Change work this is done via email to MNIT Management.

## What are the business responsibilities?

- Project Sponsorship
- End User Help Desk
- End User Training, documentation, job aids, and reference guides
- End User Communication
- Cross Functional Team Coordination
- Functional Testing

- Conduct and manage User Acceptance Testing
- Work with Business Analysts to provide knowledge, input, and documentation review
- Own business data, supporting documents, standard reports, and appropriate end user security requirements
- Set System Requirements
- Production System Functional Management
- MDHR Business and Functional Requirements and Needs Coordination
- Final product signoff for enhancement work efforts prior to production migration
- Printer management
- Monitors and other peripherals
- Fax machines and electronic faxing services
- COOP Planning for all business operations
- Work with MNIT on creation and maintenance of a Disaster Recovery Plan
- Disaster Recovery functional testing in a disaster recovery scenario

## When will regular maintenance be performed?

- Normal maintenance will be performed on agreed upon schedule

## Change Management Process/Termination

- Utilize MNIT Service Hub (Remedy) for non-development change management tracking
- Conduct regular weekly cross MDHR and MNIT team change management meetings to communicate upcoming changes to production environments

# 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.

## 1. Local Application Development and Maintenance

1. Defect rate for developed code – Target <5%
2. Application/system cost management – Target +/- 5% Budget

## 2. Local Cybersecurity

1. Number of successful intrusions – Target 0
2. Number of Sev-1/Sev-2 unresolved vulnerabilities on servers that are overdue for resolution – Target 0
3. Number of Sev-1/Sev-2 unresolved vulnerabilities on desktops that are overdue for resolution – Target 0
4. MMB Risk Scorecard value for all categories – Target >3.0
5. Annual Security Awareness Training – Target 100% MDHR staff have taken
6. Monthly Phishing Training – Target <5% fail rate

# Signature Page

Under Minnesota Statutes section 16E, the Office of MN.IT Services (dba Minnesota IT Services/MNIT) provides Information Technology services to the Agency. The Agency use of these services constitutes an acceptance of this Service Level Agreement.

The MNIT Service Level Agreement is reviewed and recognized by:

| **Agency/Entity** | **MNIT Services** |
|---|---|
| DocuSigned by: Scott Beutel 7AE6BBA0DC6A4B5... | DocuSigned by: Tarek Tomes 9BC4418FE4DE41F... |
| Scott Beutel | Tarek Tomes |
| Assistant Commissioner<br>Minnesota Department of Human Rights | State Chief Information Officer and<br>MNIT Services Commissioner |
| 10/13/2022 | 6/16/2022 |
| Date of Signature | Date of Signature |